TASK ORDER (TO)

47QFCA21F0018

Technology Synchronization of Business Operations (TSyBO)

in support of:

Department of Defense (DoD) Office of the Under Secretary of Defense (Comptroller) (OUSD(C))

Issued to:
Booz Allen Hamilton, Inc.

Conducted under Federal Acquisition Regulation (FAR) 16.505

Issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW (QF0B)
Washington, D.C. 20405

March 9, 2021

FEDSIM Project Number DE01101

Contract: **47QTCK18D0004**
Task Order: **47QFCA21F0018**
Modification P0009

B.1 GENERAL

The work shall be performed in accordance with all Sections of this Task Order (TO) and the contractor's Base Contract, under which the resulting TO will be placed. An acronym listing to support this TO is included in **Section J, Attachment B**.

B.2 CONTRACT ACCESS FEE (CAF)

The General Services Administration's (GSA) operating costs associated with the management and administration of this contract are recovered through a CAF. In accordance with the Alliant 2 base contract, the CAF shall be 0.75 percent of the total TO value with a cap of $100,000 per year per order (when order is in excess of $13.3M per order year). This TO shall have a separate Contract Line Item Number (CLIN) to cover this access fee, and this CAF shall be obligated at TO Award (TOA).

B.3 ORDER TYPES

This TO is a hybrid Cost-Plus-Award-Fee (CPAF) and Cost-Reimbursement (CR) type order.

The contractor shall perform the effort required by this TO on a CPAF basis for:

a. Mandatory Labor CLINs 0001, 1001, 2001, 3001, and 4001.

The contractor shall perform the effort required by this TO on a CR Not-to-Exceed (NTE) basis for:

a. Long-Distance Travel CLINs 0002, 1002, 2002, 3002, and 4002.
b. Tools CLINs 0003, 1003, 2003, 3003, and 4003.
c. Other Direct Costs (ODCs) CLINs 0004, 1004, 2004, 3004, and 4004.
d. CAF CLINs 0005, 1005, 2005, 3005, and 4005.

B.4 SERVICES AND PRICES/COSTS

Long-distance travel is defined as travel over 50 miles from National Capitol Region (NCR). Local travel will not be reimbursed.

The following abbreviations are used in this price schedule:

CAF	Contract Access Fee
CLIN	Contract Line Item Number
CPAF	Cost-Plus-Award-Fee
CR	Cost-Reimbursement
NTE	Not-to-Exceed
ODC	Other Direct Cost

B.4.1 BASE PERIOD:

MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
0001	Labor (Tasks 1–5)	(b) (4)		$120,658,104

CR TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
0002	Long-Distance Travel Including Indirect Handling Rate (b) (4) G&A	NTE	$450,000
0003	Tools Including Indirect Handling Rate (b) (4) MH, (b) (4) G&A	NTE	$4,300,000
0004	ODCs Including Indirect Handling Rate (b) (4) MH, (b) (4) G&A	NTE	$16,000,000

CAF

CLIN	Description		Total Ceiling Price
0005	CAF	NTE	$100,000

TOTAL CEILING BASE PERIOD CLINs: $141,508,104

B.4.2 FIRST OPTION PERIOD

MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
1001	Labor (Tasks 1- 5)	(b) (4)		$117,294,056

CR TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
1002	Long-Distance Travel Including Indirect Handling Rate (b) (4) G&A	NTE	$300,000
1003	Tools Including Indirect Handling Rate (b) (4) MH, (b) (4) G&A	NTE	$4,300,000
1004	ODCs Including Indirect Handling Rate (b) (4) MH, (b) (4) G&A	NTE	$8,000,000

CAF

CLIN	Description		Total Ceiling Price
1005	CAF	NTE	$100,000

TOTAL CEILING FIRST OPTION PERIOD CLINs: **$129,994,056**

B.4.3 SECOND OPTION PERIOD

MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
2001	Labor (Tasks 1- 5)	(b) (4)		$127,239,897

CR TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
2002	Long-Distance Travel Including Indirect Handling Rate (b) (4) G&A	NTE	$300,000
2003	Tools Including Indirect Handling Rate (b) (4) MH, (b) (4) G&A	NTE	$4,300,000
2004	ODCs Including Indirect Handling Rate (b) (4) MH, (b) (4) G&A	NTE	$8,000,000

CAF

CLIN	Description		Total Ceiling Price
2005	CAF	NTE	$100,000

TOTAL CEILING SECOND OPTION PERIOD CLINs: $139,939,897

B.4.4 THIRD OPTION PERIOD

MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
3001	Labor (Tasks 1- 5)	(b) (4)		$133,985,684

CR TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
3002	Long-Distance Travel Including Indirect Handling Rate (b) (4) G&A	NTE	$300,000
3003	Tools Including Indirect Handling Rate (b) (4) MH, (b) (4) G&A	NTE	$4,300,000
3004	ODCs Including Indirect Handling Rate (b) (4) MH, (b) (4) G&A	NTE	$8,000,000

CAF

CLIN	Description		Total Ceiling Price
3005	CAF	NTE	$100,000

TOTAL CEILING THIRD OPTION PERIOD CLINs: $146,685,684

B.4.5 FOURTH OPTION PERIOD

MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
4001	Labor (Tasks 1- 5)	(b) (4)		$111,355,004

CR TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
4002	Long-Distance Travel Including Indirect Handling Rate (b) (4) G&A	NTE	$150,000
4003	Tools Including Indirect Handling Rate (b) (4) MH, (b) (4) G&A	NTE	$4,300,000
4004	ODCs Including Indirect Handling Rate (b) (4) MH, (b) (4) G&A	NTE	$0.00

CAF

CLIN	Description		Total Ceiling Price
4005	CAF	NTE	$100,000

TOTAL CEILING FOURTH OPTION PERIOD CLINs: **$115,905,004**

GRAND TOTAL CEILING ALL CLINs: **$674,032,745**

B.5 SECTION B TABLES

B.5.1 INDIRECT/MATERIAL HANDLING RATE

Long-Distance Travel, Tools, and ODC costs incurred may be burdened with the contractor's indirect/material handling rate in accordance with the contractor's disclosed practices, provided that the base contract does not prohibit the application of indirect rate(s) on these costs.

a. If no indirect/material handling rate is allowable in accordance with the contractor's disclosed practices, no indirect/material handling rate shall be applied to or reimbursed on these costs.
b. If no rate is specified in the schedule of prices above, no indirect rate shall be applied to or reimbursed on these costs.

The indirect handling rate over the term of the TO shall not exceed the rate specified in the schedule of prices above.

B.5.2 DIRECT LABOR RATES

Labor categories proposed shall be mapped to existing GSA Alliant 2 labor categories.

B.5.3 ACCOUNTING FOR CONTRACTOR MANPOWER REPORTING

Costs associated with Accounting for Contractor Manpower Reporting, as specified in **Section C.5.1.1**, are covered in CLIN X001 and relate to this TO only.

B.6 INCREMENTAL FUNDING

B.6.1 INCREMENTAL FUNDING LIMITATION OF GOVERNMENT'S OBLIGATION

Incremental funding in the amount of **$109,515,411.00** for CLINs 0001 through 0005 is currently allotted and available for payment by the Government. Additional incremental funding for these CLINs may be allotted and available for payment by the Government as the funds become available. The estimated period of performance covered by the allotments for the mandatory CLINs is from award through **March 8, 2022**, unless otherwise noted in Section B. The TO may be modified to add funds incrementally up to the maximum of $674,032,745 over the performance period of this TO. These allotments constitute the estimated cost for the purpose of Federal Acquisition Regulation (FAR) Clause 52.232-22, Limitation of Funds, which applies to this TO on a CLIN-by-CLIN basis.

Incremental Funding Chart for CPAF

The Incremental Funding Chart Excel spreadsheet is available in **Section J, Attachment C**.

B.7 AWARD FEE RESULTS REPORTING TABLE

The Award Fee Determination Plan (AFDP) establishes award fee (**Section J, Attachment D**).

C.1 BACKGROUND

The Office of the Under Secretary of Defense (Comptroller) (OUSD(C)) is the principal staff office for the Department of Defense (DoD) on all budgetary and fiscal matters, including the development and execution of the DoD's annual budget of more than $600 billion. The Comptroller also oversees the DoD's financial policy, financial management systems, and business modernization efforts. The OUSD(C) is chair of the Financial Management Modernization Executive Committee; its goal is to ensure that each of the DoD's critical accounting, financial, and data feeder systems are compliant with applicable Federal financial management and reporting requirements. The Comptroller is also a member of the Defense Business System Management Committee.

The OUSD(C) manages the development and execution of the DoD budget with an emphasis on improving financial management across the DoD to ensure that taxpayer resources are managed wisely and efficiently. Overall, the OUSD(C) ensures that the United States (U.S.) military has the resources needed to protect and defend the U.S., its interests, and its people.

The DoD's business operations encompass many different functional areas, such as financial management, acquisition and logistics, installations and environment, and human resources management. While OUSD(C) is not specifically responsible for any of these business areas, the DoD has established senior officials who are responsible. As the leads in the business and fiscal responsibility of the DoD, the Secretary of Defense is responsible for working across the DoD functional areas to break down organizational stovepipes and create a cross-functional, end-to-end business environment that is synchronized to rapidly respond to warfighter needs in the most cost-effective way possible.

C.1.1 PURPOSE

The purpose of this TO is to provide enterprise level data to the OUSD(C), and its strategic partners (i.e., DoD Fourth Estate, DoD Departments, and IC community) as well as support in the areas of Information Technology (IT) engineering, Operations and Maintenance (O&M), technical, consulting, cyber security, and planning subject matter expertise to develop, maintain, sustain, and enhance the DoD Enterprise Government-owned data analytics environment, Advana, that includes connections to other IT supporting systems (i.e., source systems) across the DoD.

C.1.2 AGENCY MISSION

The OUSD(C) is the principal DoD officials responsible to the Secretary and Deputy Secretary of Defense for leading and enabling the management, integration, and improvement of the DoD business environment. Working across the DoD Components, the OUSD(C) is focused on delivering agile, efficient, and effective business operations that support the warfighter. This mission is implemented by leading business operations for the DoD through innovative processes and services, data-driven solutions, and mission-focused funding.

C.2 SCOPE

The contractor shall create, deliver, and maintain a cross-functional, end-to-end IT business environment that is synchronized to rapidly respond to warfighter needs in the most cost-effective way possible. The contractor shall provide full lifecycle IT support for the Advana platform including, but not limited to, product management, IT systems engineering, and development activities; user engagement activities; operational, external, and internal interface management; systems certification; mission IT engineering; metrics collection and analysis; and modeling and simulations.

C.3 CURRENT ENVIRONMENT

Information is vital to U.S. national security and the ability to understand emerging threats, project power globally, conduct operations, support diplomatic efforts, and enable global economic viability. The DoD has multiple disjointed and stove-piped information systems, distributed across modern and legacy infrastructure around the globe, leading to a litany of problems that impact warfighters', decision makers', and DoD staff's ability to organize, analyze, secure, scale, and ultimately, capitalize on critical information to make timely, data-driven decisions. Today, the DoD is largely constrained by physical resources, manpower limitations, organic skillsets and, oftentimes, laborious contracting processes to procure or grow storage and computing capabilities. In addition, the cyberspace domain continues to be an increasingly contested environment. In order for the U.S. to keep its strategic advantage, warfighters and the workforce that support them need to be provided with the proper capabilities and technologies to succeed. To this end, commercial industry has made significant strides in addressing these challenges that the DoD can leverage.

The OUSD(C) provide integration and support through the Chief Financial Officer (CFO) Data Transformation Office. They are establishing a framework to leverage commercial industry technologies for more effective management in a time of fiscal austerity, utilizing the key levers of strategy, people, process, technology, and controls. Integrated project teams are engaged to bring together the resources and capabilities of the OUSD(C) to actively work on a host of high-profile projects that will lead to significant cost savings, cost avoidance, and improved utilization of DoD capabilities for data input.

The DoD requires use of an open standards system approach, to the maximum extent practical, to achieve superior war fighting capability with reduced total operating costs. Open standards systems are expected to control development costs, provide quicker access to emergent technologies, significantly improve network performance, and reduce the costs to maintain and upgrade network systems over ever-increasing lifetimes.

In 2019, the Data Management and Analytics Steering Committee (DMASC) approved the technical architecture and the tool suite employed by a Government-developed suite of tools called Advana, to be the shared service data platform for all common enterprise data. As a shared service, Advana provides a common data platform and a suite of tools to accelerate the delivery of new analytics projects and contributes to DoD becoming a data-driven organization. This is one part of the large framework that is purpose-built to advance analytics across the DoD by

collecting enterprise data in a common place and building common data models to allow ease of access and understanding for all who require it.

C.4 OBJECTIVE

The objective of this TO is to deliver the highly specialized operational and technical expertise required to improve and strengthen OUSD(C) IT Enterprise Business Operations.

The specific outcomes for this effort are to:

a. Support the development of innovative models and tools to be integrated into existing (i.e., Advana) and new DoD systems in support of specific problems currently facing OUSD(C). It is anticipated that, these business problems will be in the functional areas of intelligence, acquisition, human resources, real property management, readiness, IT, acquisition, financial management, supply chain, logistics, policy, and warfighting operations.
b. Develop and integrate capabilities in a manner that leverages current market capabilities and emerging industry technologies.
c. Perform administrative, operational, maintenance, and programming responsibilities for the OUSD(C) IT Enterprise.
d. Provide flexibility to respond to new feature requirements as directed by the OUSD(C) or their strategic partners.
e. Enable actual capability delivery by ensuring that developed capabilities are integrated into the DoD end user environment using an agile software Development and Operations (DevOps)-centered framework for all projects.

C.5 TASKS

The following tasks are intended to cover the scope of work anticipated by the OUSD(C). Specific work products within the work scope may shift based on needs.

The contractor shall provide all expertise and services as stated in the TO to deliver the integrated technical services.

Specific tasks to be performed under the TO include:

a. Task 1 – Provide Program Management
b. Task 2 – Platform/Systems Architecture Development, Integration, and Maintenance Services
c. Task 3 – Data Science and Enterprise Analytics Services
d. Task 4 – End User Support Services
e. Task 5 – Innovative IT Technologies Research and Integration Services

C.5.1 TASK 1 – PROVIDE PROGRAM MANAGEMENT

The contractor shall provide program management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including

subcontractors, to satisfy the requirements identified in this Performance Work Statement (PWS).

In rare circumstances and unique events (e.g., new policy mandates, world events, etc.), requirements will be directed through Technical Direction Letters (TDLs) (**Section J, Attachment I**), as specified in **Section H.20**. Such TDLs, will be used to identify and track operational support needs. The Government expects that 10-15 percent of requirements will be supported through TDLs on an annual basis within a Period of Performance, consisting of various appropriation types (e.g., one-year, two-year, or no-year), depending on the bona fide need. Overarching Advana platform lifecycle and enhancement support; and program management support shall be ongoing throughout the life of the TO; a TDL will not be issued for such tasks and subtasks.

C.5.1.1 SUBTASK 1.1 – ACCOUNTING FOR CONTRACTOR MANPOWER REPORTING

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the OUSD(C) via a secure data collection site: System for Award Management (SAM). The contractor shall completely fill in all required data fields using the following web address: https://beta.sam.gov/.

Reporting inputs will be for the labor executed during the period of performance during each Government Fiscal Year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported No Later Than (NLT) October 31 of each calendar year. Contractors may direct questions to the support desk at: https://beta.sam.gov/.

Contractors may use Extensible Markup Language (XML) data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a contractor's systems to the secure website without the need for separate data entries for each required data element at the website. The specific formats for the XML direct transfer may be downloaded from the web.

C.5.1.2 SUBTASK 1.2 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a Project Kick-Off Meeting at the location approved by the Government (**Section F, Deliverable 01**). The meeting shall provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting shall provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include Key contractor Personnel, the OUSD(C) TPOC, the FEDSIM COR, and other relevant Government personnel.

At least three days prior to the Project Kick-Off Meeting, the contractor shall provide a Project Kick-Off Meeting Agenda (**Section F, Deliverable 02**) for review and approval by the FEDSIM COR and the OUSD(C)TPOC prior to finalizing. The agenda shall include, at a minimum, the following topics/deliverables:

a. Points of Contact (POCs) for all parties.

b. Personnel discussion (i.e., roles and responsibilities and lines of communication between contractor and Government).
c. Project Staffing Plan and status.
d. Transition-In Plan (**Section F, Deliverable 03**) and discussion.
e. Security discussion and requirements (i.e., building access, badges, Common Access Cards (CACs)).
f. Financial reporting and invoicing requirements.
g. Baseline Quality Management Plan (QMP) (**Section F, Deliverable 04**).
h. Earned Value Management (EVM) Plan (**Section F, Deliverable 05)**.
i. Project Management Plan (PMP) (**Section F, Deliverable 06**).
j. Project Integrated Master Schedule (IMS) (**Section F, Deliverable 07**).

The Government will provide the contractor with the number of Government participants for the Project Kick-Off Meeting, and the contractor shall provide sufficient copies of the presentation for all present.

The contractor shall draft and provide a Project Kick-Off Meeting Minutes Report (**Section F, Deliverable 08**) documenting the Project Kick-Off Meeting discussion and capturing any action items.

C.5.1.3 SUBTASK 1.3 – IMPLEMENT A TASK ORDER (TO) MANAGEMENT PORTAL SOLUTION

The contractor shall implement a TO Management Portal (**Section F, Deliverable 09**) capability that provides project management views/reporting, tracks metrics, and stores artifacts at the unclassified level. The intent of the TO Management Portal solution is to introduce efficiencies, ensure coordinated service delivery worldwide, and provide a repository for TO deliverables and artifacts. The Government seeks innovation for managing workflow processes and desires the TO Management Portal solution to possess an automated workflow process.

The contractor shall ensure the TO Management Portal solution is accessible to approved Government and contractor personnel with a .mil or a .gov account. Worldwide access to the TO Management Portal should be available to approved users. The TO Management Portal solution shall be compliant with current standards and adaptable for future DoD security standards. The contractor may use Open Source solutions and Commercial Off-the-Shelf (COTS) or Government Off-the-Shelf (GOTS) software to the maximum extent practicable.

The contractor shall provide a demonstration of the TO Management Portal at the Project Kick-Off Meeting. Once the FEDSIM COR provides the contractor with authority to proceed, the contractor shall begin implementing the approved solution in a timely and efficient manner.

At a minimum, the TO Management Portal shall provide the following:

a. Secure logical access controls with role-based views (e.g., FEDSIM COR, OUSD(C)TPOCs, and others as required).
b. A dashboard for overarching Advana platform lifecycle support activities and associated costs, and include the following:

1. Allocated budget by CLIN.
2. Funded Amount by CLIN
3. Incurred cost amount by CLIN.
4. Invoiced amount by CLIN.
5. Burn Rate by CLIN.
6. Award Fee Earned

c. A dashboard that identifies each TDL being supported, describes its associated Technical Data Package (TDP), and includes the following:
    1. TDL Identification (ID) number.
    2. Client Name.
    3. TDL Name.
    4. Abbreviated work description.
    5. Customer POC information.
    6. Contractor POC information.
    7. TDL start date.
    8. TDL end date.
    9. Allocated budget by CLIN.
    10. Funded amount by CLIN.
    11. Incurred cost amount by CLIN.
    12. Invoiced amount by CLIN.
    13. Burn Rate by CLIN and by TDL.
d. An automated workflow for Government review/approval of each Request to Initiate Purchase (RIP) (**Section J, Attachment N**), and Travel Authorization Request (TAR) (**Section J, Attachment M**), inclusive of the OUSD(C) TPOC and FEDSIM COR.
e. The ability to view financial information to allow the Government to track the financial health of each effort, including the total lifecycle support. The Government will establish the level of granularity needed at the onset of an effort (e.g., TDL, funding document, or line of accounting level).
f. An organized document library to store management-related deliverables (e.g., Monthly Status Reports (MSRs) (**Section F, Deliverable 10**), PMP (**Section F, Deliverable 06**), etc.).

The TO Management Portal solution shall be operational by the end of the transition-in period. The TO Management Portal capabilities are expected to evolve and adapt throughout the life of the TO to meet the mission needs.

C.5.1.4 SUBTASK 1.4 – PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor shall develop and provide an MSR (**Section J, Attachment F**) (**Section F, Deliverable 10**). The MSR shall not include any classified information.

At a minimum, the MSR shall include the following:

a. Activities during reporting period, by task and TDL (include ongoing activities, new activities, and activities completed, and progress to date on all above mentioned activities). Each section shall start with a brief description of the task.
b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
c. Personnel gains, losses, and status (security clearances, etc.).
d. Government actions required.
e. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
f. Summary of trips taken, or conferences attended (attach Trip Reports to the MSR for reporting period).
g. Changes to the PMP.
h. Current funding and ceiling.
i. EVM statistics.
j. Cost incurred by CLIN and TDL.
k. Accumulated invoiced cost for each CLIN and TDL up to the previous month.
l. Projected cost of each CLIN and TDL for the current month.

C.5.1.5 SUBTASK 1.5 – FINANCIAL REPORTING AND EVM PLAN

The contractor shall develop and monitor a cost sharing model to support long-term sustainment of the Data and Analytics Shared Services. The contractor shall provide reporting on return on investment for licensing costs, infrastructure, custom development, and base support and services **(Section F, Deliverable 43).**

The contractor shall employ and report on EVM in the management of this TO using a tailored plan consistent with its technical approach. The EVM Plan shall be submitted to the Government for approval (**Section F, Deliverable 05**). The contractor shall be ready to discuss its outline for the EVM Plan at the Project Kick-Off Meeting with the initial EVM Plan due **60 days** after TOA. See **Section H.10**, Earned Value Management, for the EVM guidelines.

C.5.1.6 SUBTASK 1.6 – CONVENE TECHNICAL STATUS MEETINGS

The contractor Program Manager (PM) shall convene the Technical Status Meeting monthly with the OUSD(C) TPOC, FEDSIM COR, and other Government stakeholders (**Section F, Deliverable 11**). The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. These meetings shall provide an opportunity to share lessons learned and disseminate best practices across TDLs. The contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the FEDSIM COR (**Section F, Deliverable 12**).

C.5.1.7 SUBTASK 1.7 – PREPARE AND UPDATE A PROJECT MANAGEMENT PLAN (PMP)

The contractor shall document all support requirements in a PMP and shall provide it to the Government (**Section F, Deliverable 06**).

The PMP shall:

a. Describe the proposed management approach.
b. Contain detailed Standard Operating Procedures (SOPs) for all tasks.
c. Include milestones, tasks, and subtasks required in this TO.
d. Provide for an overall Work Breakdown Structure (WBS) with a minimum of three levels and associated responsibilities and partnerships between Government organizations. The WBS shall be updated as needed and with the addition of each TDL. A WBS update does not require the re-submission of a PMP update.
e. Describe in detail the contractor's approach to risk management under this TO.
f. Describe in detail the contractor's approach to communications, including processes, procedures, communication format, and other rules of engagement between the contractor and the Government.
g. Include the contractor's QMP and EVM Plan.
h. Describe common technical architecture and custom architecture used for product development.
i. Describe interaction and reuse for technical architecture.

The PMP is an evolutionary document that shall be updated annually, at a minimum, and as project changes occur. The contractor shall work from the latest Government-approved version of the PMP.

C.5.1.8 SUBTASK 1.8 – PREPARE AND UPDATE AN INTEGRATED MASTER SCHEDULE (IMS)

The contractor shall generate and update a total lifecycle Advana IMS, including updating IMS for each product, identifying resources, establishing critical path items, and addressing schedule conflicts and risks (**Section F, Deliverable 07**). The contractor shall synchronize the IMS with other product IMS' across the program portfolio. The IMS shall be traceable to the Government provided Integrated Master Plan (IMP) events/accomplishments, and WBS.

C.5.1.9 SUBTASK 1.9 – PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report when the request for travel is submitted (**Section F, Deliverable 13**). The contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and POC at travel location. Trip reports shall also contain Government approval authority, total cost of the trip, a detailed description of the purpose of the trip, and any knowledge gained. At a minimum, Trip Reports shall be prepared with the information provided in (**Section J, Attachment G)**.

C.5.1.10 SUBTASK 1.10 – PROVIDE QUALITY MANAGEMENT

The contractor shall identify and implement its approach for providing and ensuring quality throughout its solution to meet the requirements of the TO. The contractor shall provide a QMP and maintain and update it as changes in the program processes are identified (**Section F, Deliverable 04**). The contractor's QMP shall describe the application of the appropriate methodology (i.e., quality control and/or quality assurance) for accomplishing TO performance expectations and objectives. The QMP shall describe how the appropriate methodology integrates with the Government's requirements.

The QMP shall contain, at a minimum, the following:

a. Performance monitoring methods.
b. Performance measures.
c. Approach to ensure that cost, performance, and schedule comply with task planning.
d. Methodology for continuous improvement of processes and procedures, including the identification of service metrics that can be tracked in the TO.
e. Government roles.
f. Contractor roles.
g. Methodology and tools for providing program management support, process management and control, project status and cost (including planned versus actual expenditures) reporting, and program metrics.
h. Approach to risk management, including the offeror's strategies to mitigate or eliminate risks.
i. Approach to coordinating and collaborating with other contractors to ensure risks are mitigated and a successful relationship results.

C.5.1.11 SUBTASK 1.11 – TRANSITION-IN

The contractor shall provide a Transition-In Plan (**Section F, Deliverable 03**) as required in Section F. The contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition. The contractor shall implement its Transition-In Plan NLT 30 calendar days after TOA, and all transition activities shall be completed 60 calendar days after approval of the Transition-In Plan.

C.5.1.12 SUBTASK 1.12 – TRANSITION-OUT

The contractor shall provide transition-out support when required by the Government. The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a Transition-Out Plan within six months of Project Start (PS) (**Section F, Deliverable 14**). The contractor shall review and update the Transition-Out Plan in accordance with the specifications in **Sections E and F**.

In the Transition-Out Plan, the contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

a. Project management processes.
b. POCs.
c. Location of technical and project management documentation.
d. Status of ongoing technical initiatives.
e. Appropriate contractor-to-contractor coordination to ensure a seamless transition.
f. Transition of Key Personnel roles and responsibilities.
g. Schedules and milestones.
h. Schedule for product backlog prioritization and sprint planning meetings with specific dates and frequency.
i. Actions required of the Government.

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings or as often as necessary to ensure a seamless transition-out.

The contractor shall implement its Transition-Out Plan NLT six months prior to expiration of the TO.

C.5.1.13 SUBTASK 1.13 – PROGRAM OF RECORD (PoR) TRANSITION ROADMAP

The contractor shall prepare and update a PoR Transition Roadmap for each product developed under the TO (**Section F, Deliverable 16**). The roadmap shall define the targeted deployment location, timeline, and all development milestones from product inception to fielding.

C.5.2 TASK 2 – PLATFORM/SYSTEMS ARCHITECTURE DEVELOPMENT, INTEGRATION, AND MAINTENANCE SERVICES

The contractor shall provide comprehensive IT development, configuration, maintenance, and cybersecurity support for the OUSD(C)IT Enterprise for the Advana analytic environment and connections to other supporting DoD analytic IT environments (i.e., source systems). The contractor shall provide full-scope system, application, network, storage, and security management support. It shall also provide integration and maintenance support for new and existing features, functions, content, and components of the OUSD(C)IT Enterprise environment and the Advana analytics environment. In addition, the contractor shall develop a process for proposing, vetting, and executing future products within the existing product lines and any product lines that are developed under this TO for Advana and other supporting DoD analytics environments (**Section F, Deliverable 17**).

C.5.2.1 SUBTASK 2.1 – DEVELOPMENT AND IT ENGINEERING SUPPORT SERVICES

The contractor shall identify and apply modern Development, Security, and Operations (DevSecOps) best practices that provide for secure and continuous development, test, and operations activities. The contractor shall establish a continuous integration, delivery, and user feedback methodology resulting in systematic, repeatable, secure, and streamlined delivery of capabilities to the production environments. The contractor shall comply with the DoD

Enterprise DevSecOps Reference Design, where possible, and notify the OUSD(C) TPOC and FEDSIM COR in writing otherwise.

The contractor shall provide development support including architecture support, systems engineering, software engineering development and integration, algorithm development, security planning and compliance (including achieving Authority to Operate (ATO)), system level testing, and innovation development and implementation. Additional contractor support shall include the following:

a. Identifying web and data applications that require replatforming, reengineering, or infrastructure support and fit within the mission and function of the OUSD(C).
b. IT architecture and engineering support.
c. Supporting the integration, development, testing, and deployment of enterprise data analytics applications within the security boundary of the OUSD(C)solutions, assuming operational control where needed.
d. Integrating applications using a common security framework, operational workflow, and toolsets, without impacting tangential accreditations across DoD networks and solutions.
e. Enabling the ability to integrate and test COTS/GOTS products (as an entire solution or as part of an overall system solution).
f. Enabling the ability to quickly augment and enhance existing tools, applications, and methodologies to advance analytic efforts and maintain currency with changing terrorism milieu.
g. Providing technical advice and engineering guidance for next-generation planning efforts, including integration with other enterprise services.
h. Providing system initialization, deployment, accreditation, and system administration functions for all unclassified and classified Artificial Intelligence (AI) model containers.
i. Developing the necessary Transition Planning including user training, support staff training, and any applicable decommissioning activities for systems/services that have been replaced or enhanced (**Section F, Deliverable 18**).
j. Supporting IT architecture and engineering for IT Enterprise Continuity of Operations (COOP)/Disaster Recovery (DR), and service availability.
k. Planning and implementing mission capabilities and transitioning to enterprise services, virtualized, and cloud-based technologies.
l. Developing, deploying and maintaining fully automated data pipelines in accordance with all applicable DoD IT control standards.

The contractor shall maintain flexibility for both a cloud and hybrid cloud approach in all migration of data, infrastructure, and application development. The contractor shall support strategic partner requests and priorities and research, design, and prototype solutions to store, rapidly access, analyze, and maintain data sets to be used within customized application workflows, dashboards, and interactive data visualizations.

The contractor shall provide comprehensive documentation and information necessary to monitor the DevSecOps processes, procedures, and/or policies that were implemented in the creation of the applications (**Section F, Deliverable 20**).

C.5.2.1.1 SUBTASK 2.1.1 –SYSTEMS AND SOFTWARE DEVELOPMENT

The support provided by the contractor shall cover the entire IT engineering lifecycle including requirements gathering, system design and development, installation, integration and testing, and sustainment. The contractor shall use agile methodologies for software development, where the development is organized into one or more releases consisting of multiple sprints. The contractor shall develop, deploy and maintain fully automated DevSecOps solution. The contractor shall define the frequencies and durations of the releases and sprints during project planning and submit for approval by the OUSD(C)TPOCs. The contractor shall provide weekly progress updates and demonstrations to the Government and update the contractor schedule for the Weekly Status Report (WSR) (**Section F, Deliverable 21**).

During project planning, the contractor shall define team structure, development environment, system requirements, and mission interaction; and, the contractor shall review the architectural specification, high-level system design, and current supporting processes. The contractor shall deliver a Development Sprint Plan to document the design approach, agile code development, integration, test, quality, and configuration control processes and procedures that will be utilized in the project, involving mission elements to verify design, functionality, and implementation plans (**Section F, Deliverable 22**).

The contractor shall coordinate with the Government, as required, during project preparation or development sprints for the performance of tasks including:

a. Identifying and setting up all necessary tools to support the development and management activities.
b. Identifying processes and plans for mission interaction to understand mission needs, gather requirements, validate design and planning implementation, acquire feedback, and deliver products and capabilities commensurate with mission needs and priorities.
c. Establishing the most effective agile framework.
d. Defining processes such as code control, daily builds, and regression tests.
e. Defining or updating processes and procedures for configuration control.
f. Coordinating with IT security and preparing or updating security-related documentation.
g. Setting up and testing the integrated development environment and other development tools.
h. Defining processes for documenting user stories, business priorities, and planned enhancements with the estimated effort for each requirement.
i. Producing or updating the interface control document and interface design document(s) to identify and characterize all the external interfaces.
j. Producing or updating the System Design Document (SDD), including system architecture design and the design of external interfaces to be extensible and scalable (**Section F, Deliverable 23**).
k. Producing or updating the Database Design Document (DBDD) and documenting the logical database schema (**Section F, Deliverable 24**).
l. Producing or updating the Test and Evaluation Master Plan (TEMP) (**Section F, Deliverable 25**).

m. Identifying the list of software tools, licenses, and hardware needed by the team for development and documentation in the Bill of Materials (BOM) (**Section F, Deliverable 26**).
n. Producing or updating the User Training Plan (**Section F, Deliverable 27**).

The contractor shall provide portfolio backlog planning to support the Government's long-range program objectives. The contractor shall develop a Release Plan based on product backlog priorities set by the Government and aligned with a product roadmap that documents the schedule and contents of proposed system releases for deployment (**Section F, Deliverable 28**). The contractor shall coordinate with the Government and update the release plan prior to each release deployment.

The contractor shall coordinate with the Government and conduct sprint planning meetings to plan each sprint based on backlog priorities, estimated effort required, and scope and resources available during the sprint. The contractor shall document the planned requirements for the sprint in the sprint backlog.

In conducting agile sprints, the contractor shall complete tasks including:

a. Defining the schedule for all agile ceremonies and providing it to the Government for attendance, depending upon availability.
b. Designing and coding the system to meet the requirements documented in the sprint backlog.
c. Demonstrating each sprint release to the Government and mission owner for approval to deploy to the testing environment.
d. Developing the system and interface test procedures, test cases, and test data in accordance with the TEMP. The test procedures shall include test pre-conditions, test sequences, and anticipated results/assertions.
e. Updating the Requirements Traceability Matrix (**Section F, Deliverable 29**).
f. Performing functional tests and documenting the test results. The functional tests shall address the verification that all requirements, specified in the sprint backlog, have been met.
g. Conducting a sprint review/retrospective on the final day of the sprint, including final accounting of user stories planned, completed, added, and deferred with demonstrations of functionality completed during the sprint.

The contractor shall conduct a sprint review to update and re-prioritize a product/change request/development requests backlog based on Government direction and as appropriate. The sprint review shall include reviewing technical details of features developed in the sprint, documenting lessons learned, documenting development metrics, and updating a product backlog, as required. A summary of the results of the sprint review that identifies the technical accomplishments of the sprint cycle shall be documented in a Sprint Summary Report and described in non-technical terms (**Section F, Deliverable 30**). The Sprint Summary Report shall include user stories as well as planned, completed, added, and deferred results.

C.5.2.2 SUBTASK 2.2 – SYSTEM AND DATA MIGRATION

The contractor shall provide system and data migration from the OUSD(C) development environments to the deployment environments (e.g., Advana or other data analytics environments), including:

a. Preparing a System Migration Plan to document plans for migrating data, application containers, and system operation and integrating new components into existing programs or replacing programs (**Section F, Deliverable 31**).
b. Preparing migration procedures that describe the steps and activities required to complete migration (**Section F, Deliverable 32**).
c. Developing back-out procedures required for returning the application to a previous operational state, in the event a difficulty is encountered in one or more steps during the migration (**Section F, Deliverable 33**).
d. Building and implementing the migration solution.
e. Migrating data from authoritative data sources to the Advana or another analytics environment, as directed by the Government.

C.5.2.3 SUBTASK 2.3 – SYSTEMS INTEGRATION

The contractor's system integration approach shall support the rapid and efficient insertion and refreshment of technology through a modular design and use of open standards and open interfaces. The contractor, in conjunction with the Government, shall define the functional partitioning and the physical modularity of the system to facilitate future replacement of specific subsystems and components by third parties without impacting other parts of the system.

The system integration architecture shall minimize inter-component dependencies to allow components to be decoupled. Specifically, the contractor's integration approach shall result in modules that have minimal dependencies on other modules (loose coupling) with widely accepted and well-defined standards-based interfaces and the absence of undocumented data sharing or service calls. The contractor shall specify, publish, and maintain widely accepted and well-supported open standard interfaces for all modular integration. The purpose is to ensure that any changes to one module will not necessitate extensive changes to other modules and, hence, facilitate module replacement and system enhancement. The contractor shall describe its approach to determine the level of coupling and the design trade-off approach. Additionally, the contractor shall be responsible for system-wide data mapping and data management services, which include the facilitation, orchestration, and management of a multi-faceted data environment (potentially polyglot/multi-model) and optimizing the data environment to support scalability and performance.

The contractor shall provide the Government information needed to support third-party development and delivery of competitive alternatives of design for software or other components or modules on an ongoing basis (**Section F, Deliverable 34**). The contractor shall also work closely with the Government and third-party providers to maximize module re-use and determine how to best leverage system and module services by enabling those capabilities to be broadly available to other developers and identifying any issues with scalability, latency, licenses, or other issues that could interfere with the efficient use of a service. At the same time, the

contractor shall respect and work to protect all intellectual property rights of third party providers through Associate Contractor Agreements (ACA) as defined in **Section H.19.**

The contractor shall provide systems integration services, including:

a. Identifying component subsystems of the overall system and determining the requirements for ensuring that the subsystems work together to function as a single system, including integration paths for partner agency data, both regularly shared and ad-hoc in nature, to enable rapid exposure to analysts.
b. Planning, documenting, and maintaining solutions to total systems or subsystems that use internally created and/or COTS products (**Section F, Deliverable 35**).
c. Providing a Total System Perspective including relationships, dependencies, and requirements of hardware and software components (**Section F, Deliverable 36**).
d. Researching COTS and GOTS solutions to solve integration problems and/or meet system requirements.
e. Ensuring that the mission applications/tools, web systems, and portals integrate effectively with existing enterprise systems and data stores with the goal of maintaining a well-connected, secured, and controlled enterprise of systems that maintains high systems availability with rapid development and exposure to analysts.
f. Ensuring service development follows the structured development, test, and release management processes in addition to stringent change management and configuration control. Identifying, developing, coordinating, maintaining, delivering, and updating required interface specifications, including the definition of services, data flows, and dependencies for internal and external service providers.
g. Integrating and optimizing workflow, automation, manual processes (where necessary), and feedback loops across the DevSecOps environment and with mission owner elements to enable automated, continuous capability delivery to mission.

C.5.2.4 SUBTASK 2.4 – TESTING SERVICES

The contractor shall provide Test and Evaluation (T&E) services of the data models against metrics determined prior to model development and testing of the final integrated product. Where possible, the activities shall be answered within the agile development framework for system development in conjunction with the OUSD(C) T&E team. For data models, T&E will occur once selected models are promoted for use, to ensure the model meets all defined metrics.

During testing, the contractor shall engage with the end-user community and designated representatives (e.g., proxies and testers) on a frequent basis. Development and testing shall include use of automated regression test techniques as part of a Continuous Integrations (CI)/Continuous Development (CD) process.

The contractor shall provide engineering support required to review, assess, and analyze all levels of system documentation to identify and define test requirements. The contractor shall provide Requirements Traceability and Change Impact Assessments in close coordination with the OUSD(C) T&E team (**Section F, Deliverable 37**). The contractor shall conduct unit and integration testing prior to delivery, but T&E will be conducted through the OUSD(C) T&E team

with outside support, if necessary. The contractor shall develop, deploy and maintain automated T&E. The OUSD(C) is striving for full testing automation.

The contractor shall evaluate test coverage with respect to test type, test validity, test scenarios, test conduct, test results, and problem report content. The goal is to reduce the number of defects or problems reported upon integration into operational Enterprise IT platform systems using AI capabilities for continually improving software verification level test methods.

The contractor shall plan, conduct, participate, and execute T&E activities including:

a. Developing, revising, and maintaining Test Plans (including security test plans) in coordination with the OUSD(C) T&E team (**Section F, Deliverable 38**).
b. Preparing Security Test Procedures (**Section F, Deliverable 58**) and Security Test Reports (**Section F, Deliverable 59**) specific to any of the AI/ Machine Learning (ML) models and Application Program Interfaces (APIs) produced.
c. Updating the test plans to reflect changes to existing tests due to enhancements or deficiency corrections.
d. Preparing the test environment, including the setup and breakdown of test equipment and systems.
e. Executing tests according to the test plans and test procedures and collecting test data.
f. Documenting deficiencies via Problem Reports (PRs) and providing a Final Test Report (**Section F, Deliverable 39**).

The contractor shall analyze test data and perform the following:

a. Provide a Deficiencies Assessment of deficiencies uncovered during testing including support of root cause analysis and solution recommendations (**Section F, Deliverable 40**).
b. Provide a Test Procedure Improvements Recommendation to facilitate improved deficiency detection (**Section F, Deliverable 41**).
c. Assess the impact to other system components of deficiencies uncovered during testing.
d. Perform Trade-off and Analysis of Alternatives Assessments (**Section F, Deliverable 42**).
e. Provide test artifacts, objective quality evidence, and detailed analysis results.
f. Document user feedback for incorporation into future development actions.

The contractor shall conduct, participate, or provide witness in system T&E, certification, and training events to be held at Government or non-Government venues, as needed. Events shall include the following:

a. Developer/Capability Test.
b. Integrated Software/System Level Test.
c. Formal Qualification Test (FQT).
d. Verification and Validation (V&V) Test.
e. Software Build FQT.
f. Segment/System Test.

C.5.2.4.1 SUBTASK 2.4.1 – TEST ENVIRONMENT

The contractor shall sustain a Government provided enterprise test environment that is representative of all production environment systems in order to facilitate Government-specific test and validation requirements, training, and evaluation.

All source code evaluation, scanning, and testing (e.g., function security, load, performance, etc.) shall be conducted within the test environment. The contractor shall not use proprietary code without express written approval from the Government. The contractor shall address any issues encountered during installation of test media or test execution, and it shall resolve any problems with the applications. For the majority of testing, OUSD(C) requires the use of the Government-provided test environment; however, in certain circumstance (as directed by the Government), the contractor may be required to provide a development and integration environment under this TO. In such event, the associated development shall be performed at the contractor's isolated development environment. A development, integration, and test environment, if required, shall accommodate rapid development and enterprise-wide implementation.

The contractor shall provide media for all source code, installation kits, software, and documentation. It shall include those related to architecture, test design, test results, and installation procedures, and it shall build procedures/scripts in a secure manner at the end of each update.

C.5.2.5 SUBTASK 2.5 – OPERATIONS AND MAINTENANCE (O&M)

The contractor shall provide support to sustain and operate system(s). The contractor shall perform general O&M, troubleshooting, and repair of Advana platform and existing connections to source systems.

The contractor shall coordinate with the Government and implement a system/software Lifecycle Management Process (**Section F, Deliverable 19**) to achieve a single lifecycle for the program. It shall include planning, designing, developing, integrating, and testing verification and validation activities applicable to both enhancement of current technologies and creation of new capabilities that include automation, data science, big data analytics, data ingestion and manipulation, Software Development Kit (SDK), ML, AI, elastic computing, emerging/emergent technologies, Publicly Available Information (PAI) exploitation, social network analysis, alerting and warning, and advancing traditional analytic methods.

The contractor shall modify application software and systems to include corrective maintenance, preventative maintenance, and modifications needed to meet new user requirements, changes in underlying design, or aging system or architecture issues. In addition, the contractor shall install and configure automated tools to track network configuration; monitor status and performance; detect, diagnose, and resolve network problems; and project future capacity requirements.

The contractor shall provide O&M support to a Government-owned commercial cloud service provider environment. This will be a Government-owned account procured, through the ODC CLIN of this TO, and administered by the contractor on behalf of the Government.

C.5.2.6 SUBTASK 2.6 – OTHER ENGINEERING SERVICES

C.5.2.6.1 SUBTASK 2.6.1 – DATA OPERATIONS AND GOVERNANCE

The contractor shall provide data operations and governance within this TO including developing data access workflows, integrating new tools and capabilities, and providing capacity management, Configuration Management (CM), and automation. This shall include continuous evaluation of the effectiveness, cost, and performance of the infrastructure to provide analytic capability to a growing user population and increasingly complex data analytic capability.

The contractor shall be responsible for maintaining high throughput through a continuous reliable data pipeline and automated data ingest capability, demonstrating the capability to identify source data, allocate high-priority data systems, configuration items, and risks. The contractor shall also track data requests and provide weekly status updates on progress.

The contractor shall coordinate with user stakeholders to influence data planning processes and with functional stakeholders to prioritize high-value data streams. The contractor shall be responsible for providing expertise and input in working with various data providers and data transport mechanisms such as direct connect to source systems, File Transfer Protocol/Secure File Transfer Protocol (FTP/SFTP), and Representational State Transfer (REST) API Coordination efforts to support existing and future Memorandum of Agreements (MOAs) (**Section F, Deliverable 45**), enabling compliant and consistent data feeds as part of automating data pulls from source systems.

The contractor shall develop standard analytic data models, linkages, metadata, and definitions; validate received data transformed against known business rules and data structures; and coordinate with stakeholders to gain acceptance. The contractor shall provision tools to safeguard the information base of an environment using a comprehensive security model, ensure users have unaltered roles and permissions ascribed, and ensure the system unequivocally enforces these roles and permissions. The contractor shall be responsible for reporting monthly on data quality issues impacting IT portfolio decision making at the enterprise level (**Section F, Deliverable 46**) and developing and curating a data catalog for improved discoverability and understandability of data, encouraging a collaborative environment (**Section F, Deliverable 47**). The contractor shall also be responsible for insurance of governance controls to support Personally Identifiable Information (PII), Protected Health Information (PHI), and Business Sensitive and Classified Data.

The contractor shall support the development of an automated data pipeline, data storage, and data access capabilities that will support the integration and loading of new data sets, perform basic transformations, perform metadata tagging, and provide visual metrics and reports. The contractor shall automate Quality Assurance (QA) of data feeds, provide detailed logging information, and automate routing of incomplete records as to not disrupt the pipeline. The contractor shall continuously research, design, and prototype custom and off-the-shelf software (i.e., COTS and/or GOTS) and methods to identify trends and report on technological advancements supporting automated data ingest, data fusion and transformation, data storage, data access, analytics, and data security across DoD functional areas.

The contractor shall also provide the following services:

a. Develop API for data availability to the enterprise (**Section F, Deliverable 48**).
b. Develop strategies for persistent advanced analytics on data ingest.
c. Promote self-service analytics by enabling user defined data ingest in line with platform-approved governance models, security, and data quality and provide data operations consulting services for stakeholders and organizations that require it.
d. Develop data sandbox environments for user or organization-specific analytics.
e. Develop, update, integrate, and maintain a suite of tools to support data discoverability, understandability, transformation, analysis, and usability (**Section F, Deliverable 49**).
f. Perform, build, or buy analysis for financial feasibility, research, and development of new capabilities and maintain and extend the data.mil homepage and integrated components.

C.5.2.6.2 SUBTASK 2.6.2 – CONFIGURATION MANAGEMENT (CM) SUPPORT

The contractor shall develop, maintain, update, and implement CI; control configuration baselines; and conduct functional and physical configuration audits. CM may include non-IT assets, work products used to develop the services, and CIs required to support the services that are not formally classified as assets. The contractor shall provide a CM Plan **(Section F, Deliverable 50).** The contractor shall provide the following CM support:

a. Ensure systems compliance with DoD standards and documented reference models.
b. Ensure integrity between business requirements and CIs by maintaining an accurate and complete CM system.
c. Ensure all systems changes are documented against current systems baselines and satisfy validated requirements.
d. Maintain operational level configuration items including application documentation, training materials, system design documentation, and/or application operation startup/power down procedures.
e. Establish and maintain program and project-level CM technical data repositories tracking Engineering Change Proposals (ECPs), PRs, Requests for Waivers (RFWs), Requests for Deviations (RFDs), Specification Change Notices (SCNs), Notice of Revisions (NORs), and other configuration item data and requests. The contractor shall maintain and operate web-based CM server repositories.
f. Establish appropriate authorization controls for modifying CIs and verifying compliance with software licensing.

C.5.2.6.3 SUBTASK 2.6.3 – CYBERSECURITY SUPPORT SERVICES

The contractor shall implement and maintain all aspects of cybersecurity engineering support in accordance with all Federal, DoD, and agency-specific security initiatives. The contractor shall implement all phases and aspects of the DoD accreditation/certification policies and procedures for DoD IT during the entire lifecycle for all systems and environments. The contractor shall evaluate, identify, and implement innovative cybersecurity practices and tools to enable the Government to meet security standards with the greatest possible efficiency.

The contractor shall:

a. Incorporate evolving cybersecurity requirements and emerging technologies to comply with the DoD Architectural Framework (DoDAF).
b. Support cybersecurity-related administration tasks, including providing system remediation and configuration and developing Assessment and Authorization (A&A) documentation
c. Maintain the platform/systems to meet requirements for certificate-based authentication (i.e., CAC and Public Key Infrastructure (PKI)) and integration with DoD enterprise authentication policies, procedures, and systems.
d. Support DoD standards for A&A processes and procedures (e.g., Risk Management Framework (RMF) and Platform IT (PIT)).
e. Implement and validate Security Technical Implementation Guideline (STIG) requirements, installation checklists, and other security process requirements.
f. Maintain a high state of cybersecurity compliance and operational availability by monitoring and applying all applicable STIGs and patches within the mandated implementation period for the Advana and OUSD(C) systems.
g. Provide technical support for Statement on Standards for Attestation Engagements (SSAE)-18 audit.
h. Conduct annual cybersecurity assessments or support a third-party assessment to evaluate Advana's ability to meet cyber risk management standards and frameworks.

C.5.2.6.4 SUBTASK 2.6.4 – PROVIDE COOP/DR IT SUPPORT

The contractor shall provide IT support to OUSD(C) with COOP/DR efforts. The contractor shall accomplish failover testing to internal backup systems and external replication sites. To meet the failover testing requirement, the contractor shall prepare and maintain COOP and DR operations artifacts.

C.5.3 TASK 3 – DATA SCIENCE AND ENTERPRISE ANALYTICS

The contractor shall provide data operations and governance within the Advana platform or other supporting analytics environments as directed by the Government. At a minimum the contractor shall be responsible for:

a. Deploying analytical concepts and AI solutions into a usable, demonstrable, full-stack capability and providing a unique combination of expertise, data science exploration, algorithm development, statistical model validation, stakeholder verification of mission impact, and solution operationalization.
b. Employing multiple agile teams with multidisciplinary skillsets across the variety of business domain challenges and leveraging use case teams comprised of data scientists, software developers, production analysts, and software testers. The contractor shall also optimize prototypes and convert proven ideas into robust capabilities for delivery.
c. Delivering on-demand data science capability to allow DoD organizations to continuously and persistently leverage data science to positively impact the operating mission, leveraging a team comprised of both highly experienced data science experts

and functional expertise with deep rooted knowledge of the business domain, mission space, and data.

d. Obtaining, integrating, cleaning, and preparing data for analysis from a wide variety of sources and formats, and exploring, analyzing, and summarizing large, diverse datasets through multiple techniques (e.g., visualizations and interactive dashboards) to enable decision making. The contractor shall demonstrate the ability to work with and handle information assets characterized by a high volume, velocity, variety, and/or veracity that require technology that employs massively parallel processing to deliver insights into the data.
e. Performing statistical learning and pattern recognition through unsupervised, supervised, and reinforcement learning methods.
f. Leveraging deep learning techniques/technologies such as neural networks/Graphical Processing Units (GPUs) to gain unique insights consistent with the Joint Artificial Intelligence Center (JAIC) guidelines and support Robotic Process Automation.
g. Researching data fusion efforts that may include the receipt, storage, analysis, and protection of PII or PHI of DoD military and civilian personnel and military personnel dependents (**Section F, Deliverable 80**).
h. Researching an enterprise-wide data integration environment to address DoD information analysis. This research shall develop and provide the data platform and analytical tools for authorized DoD Office of People Analytics; Defense Manpower Data Center; and Military Department staff officers, researchers, and analysts to discover and connect data and produce actionable policy and program insights (**Section F, Deliverable 81)**.
i. Providing data model support for user-defined data structures, schemas, and data ingest capabilities. The contractor shall ensure data ingested does not violate existing PII, PHI, Business Sensitive, and Classified data exposure policies and implement guardrails and automated checks to prevent data spillage.
j. Developing Secure API mechanisms for users to develop machine to machine interfaces to retrieve data for external application use (**Section F, Deliverable 60**).
k. Providing tools, applications, and training for users to conduct independent assessment of data under their control and explore, analyze, export, and publish insights they create with the data.
l. Creating prototypes/proof of concept demonstrations utilizing rapid development of new data pipelines that can be used for future, more frequent, automated data feeds.
m. Coordinating with functional and technical stakeholders to define methods for enriching, aggregating, and exposing data in a curated form to support analytics at scale in support of the prototype use cases.
n. Researching and defining master data management techniques to centrally manage lookup tables, business glossaries, and data profile information.
o. Deploying validated models into production to support the development of decision support tools, dashboards, workflows, and munitions related use cases.
p. Implementing auditable controls that prohibit users from updating, deleting, accessing, viewing, or otherwise manipulating data that is outside their explicit control.

C.5.4 TASK 4 – END USER SUPPORT SERVICES

The contractor shall ensure that the platforms/systems are in line with the needs and specific requirements of the user population and ultimately improve human interface of the systems/platforms. Requirements of this subtask may include, but are not limited to, evaluation of future needs and trends, user-centered design, rapid prototyping, development, testing, and deployment. The contractor shall provide training and end-user support on existing and newly integrated products. This support shall be tailored by the contractor on a product-by-product basis with direction from the Government and documented in the PMP for the product (**Section F, Deliverable 61**). The contractor shall leverage new training methods and technologies in order to replace existing, in-person classroom training. The contractor shall ensure users are able to learn a system properly and employ the system through the simplification of the user interface. Gaps in intuitive learning shall be augmented by innovative solutions including searchable message boards, chats with experts, and in-software help widgets. The contractor shall support all data product customer-support tasks in both Continental United States (CONUS) and Outside CONUS (OCONUS) locations.

C.5.4.1 SUBTASK 4.1 – SYSTEM AND USER SUPPORT

The contractor shall continuously evaluate and update the users' experience and user interface as necessary. The contractor shall provide system and end-user support on a product-by-product basis. These services shall be included in the PMP for the product in concert with the deployment and sustainment stakeholder engagement. As part of this subtask the contractor shall provide:

a. Outreach and relationship management, which includes:
    1. Collecting community/user feedback and analyze and assess results to provide recommendations for continuous systems improvement (**Section F, Deliverable 53**).
    2. Designing and testing hardware and software user interfaces to optimize user performance and reduce the likelihood of user errors (**Section F, Deliverable 54**). The designs shall be compatible with user capability and limitations.
    3. Developing, maintaining, and executing user training materials on a per product basis (**Section F, Deliverable 62**) and user outreach plans (**Section F, Deliverable 51**).
    4. Providing continuous user/stakeholder engagement to gather user feedback, introduce new features, and answer frequently asked questions. As part to of user engagement activities, the contractor may be required to attend conferences, panel discussions, and other engagement events to promote and further the use of analytics and enterprise insights and development of tools across the enterprise.
    5. Developing automation, guided workflows, web-based tutorials, and self-help (where appropriate) for user onboarding and new users.
b. Business planning and a full spectrum of requirements management services, which includes:
    1. Translating business needs into actionable requirements.

2. Engaging OUSD(C) on emerging business needs and develop business cases of potential solutions.
3. Analyzing, proposing, and matching business and user needs with new or currently available technologies for end-users.
4. Purchasing, monitoring, negotiating, and evaluating enterprise licenses for essential COTS tools.

c. Monitoring and event management services, which includes:
   1. Continuously monitoring and managing the health and performance of the system/network. The enterprise monitoring and event management solution shall meet all policies and mandates for system security, including the ATO.
   2. Continually identifying opportunities to enhance monitoring with new integration and capabilities and employ self-healing techniques for remediation.
   3. Developing proactive strategies and automations (where applicable) to prevent, detect, and remediate service impacting issues and improve overall incident response efficiency (**Section F, Deliverable 68**).
   4. Continuously monitoring the network and supporting infrastructure for breaches, logs, and tracking events.
   5. Escalating events, when applicable, to incidents or problems and record when they are address and closed.
   6. Utilizing ML to monitor, analyze, assess, and review audit trails, logs, and other information collected to identify network/system events that may constitute violations of system security.

d. Access management, which includes:
   1. Recommending and implementing an access management process that establishes processes and creates and maintains user accounts for mission applications (**Section F, Deliverable 67**).
   2. Establishing and maintaining account management using Role-Based Access Control (RBAC) for systems access including user accounts for prototypes and developmental systems.

e. Request fulfilment, which includes:
   1. Developing a service catalog to advertise capabilities across the enterprise to support simplified inter-agency transactions and cost sharing (**Section F, Deliverable 44**).
   2. Recommending and implementing a request fulfillment process that responds to user requests in a timely and efficient manner (**Section F, Deliverable 69**).

f. Incident, problem, and outages management, which includes:
   1. Accurately detecting and responding to incidents, problems, outages, and security threats across the enterprise systems and providing intelligent insights that enable quick response measures to reduce the impact of incidents and proactively prevent future incidents.
   2. Recommending and implementing an incident management process (**Section F, Deliverable 70**) and monitoring the infrastructure and capabilities for emerging

and actual incidents, problems, outages, and other events impacting IT performance.

3. Fixing faults and restoring services.
4. Providing preventative mitigations to faults and service degradations, where possible, through proactive measures to address service degradation or interruption for users (**Section F, Deliverable 70**).
5. Providing a proactive problem management process (**Section F, Deliverable 71**) that includes measures of error prevention, trend analyses, actions and measures, and preparation of quality reports (**Section F, Deliverable 72**).
6. Supporting the Government's development of an automated dashboard showing the status of the network and system performance, security compliance, and other metrics as requested by the Government.
7. Providing problem management during normal business hours (8:00 a.m. Eastern Time (ET) – 5:00 p.m. ET) with a response (e.g., phone, email, chat, as applicable) during non-standard hours (i.e., after hours, weekends and Federal holidays), no later than 24 hours after problem identification.

C.5.4.2 SUBTASK 4.2 – TIERS 1, 2, AND 3 CUSTOMER ASSISTANCE SUPPORT

The work to be performed under this task encompasses full spectrum Tiers 1, 2, and 3 Customer Assistance Support. The contractor shall implement processes that clearly demonstrate how information will flow through one individual until customer satisfaction is achieved. The contractor shall provide status updates and reports as required for the Tiers 1, 2, and 3 Customer Assistance Support activities utilizing a monthly report summarizing activities completed for this subtask (**Section F, Deliverable 73**). Specifically, the contractor shall:

a. Develop an SOP for Tiers 1, 2, and 3 customer assistance operations within 60 calendar days of PS and update it bi-annually (**Section F, Deliverable 74**).
b. Provide Tier 1 live-person customer assistance and support services for OUSD(C)'s websites, systems, and applications 24 hours a day, seven days a week, and 365 days a year (24/7/365).
c. Provide 24/7/365 Tier 2 IT support when required to investigate and troubleshoot non-technical issues.
d. Provide 24/7/365 Tier 2 and Tier 3 IT engineering support when required to investigate and troubleshoot issues.
e. Acknowledge receipt of all customer assistance requests within two hours.
f. Notify users of system outages and establish/maintain a business process to ensure any system outages, scheduled or not, are known and conveyed to users.
g. Perform account maintenance and setup activities, including creating, modifying, and/or deleting user accounts in support of OUSD(C) account maintenance SOPs within 60 days of PS and quarterly thereafter.
h. Assist users in gaining access to their existing accounts (e.g., resets and lockouts).
i. Develop and maintain a Tier 0 (self-service) knowledge base to allow for rapid lookups of common issues within 60 days of PS and update it monthly.

j. Analyze and recommend improvements to OUSD(C) customer support methodologies.
k. Prepare and submit monthly customer assistance and support metrics reports including the number of support queries received, resolved, and pending and a summary of the top ten help trends (**Section F, Deliverable 75**).

C.5.5 TASK 5 –INNOVATIVE IT TECHNOLOGIES RESEARCH AND INTEGRATION

The contractor shall analyze and review the latest advances in IA technology including commercial, non-commercial, and GOTS solutions and industry best practices to optimize the current systems. The contractor shall facilitate connections with industry, academia, and startups to capture new inspiration, ideas, and partnerships that address long- and short-term mission critical needs. The contractor shall develop a process to implement the Government-approved initiatives to be compliant with all applicable DoD processes and policy. The approach shall define both holistic and incremental processes for achieving the approved/required capability and at a minimum perform the following:

a. **Analysis**: The contractor shall provide analysis of the emergent and emerging technologies and/or process (**Section F, Deliverable 76**). The contractor shall assess the current platform baseline, identify opportunities for improvement including recommendations for software and services (**Section F, Deliverable 77**), and provide recommendations for implementing innovations. The contractor shall clearly identify any risks associated with the recommendations. Based on the contractor's analysis and applicability of the latest advances in technology to the analytics environment, the Government will determine when and if a particular innovation support is required.
b. **Prototype (if applicable) and Design**: The contractor shall provide detailed design in accordance with the concept of operations (CONOPs), including cybersecurity and migration strategies (**Section F, Deliverable 52**). The contractor shall provide Test Strategy and test execution. The contractor shall deliver prototype/proof of concept (when applicable).
c. Monitor and Report Innovation Results (Section F, Deliverable 55): The contractor shall provide qualitative and quantitative results comparing the planned benefits identified in the Analysis to the actual benefits achieved.

This page intentionally left blank.

E.1 PLACE OF INSPECTION AND ACCEPTANCE

Inspection and acceptance of all work performance, reports, and other deliverables under this TO will be performed in the NCR by the FEDSIM COR and OUSD(C) TPOC.

E.2 SCOPE OF INSPECTION

All deliverables will be inspected for content, completeness, accuracy, and conformance to TO requirements by the FEDSIM COR and OUSD(C)TPOC. Inspection may include validation of information or software through the use of automated tools, testing, or inspections of the deliverables, as specified in the TO. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality, and adequacy of all deliverables.

The Government requires a period NTE 15 workdays (unless specified otherwise in **Section F**) after receipt of deliverable items for inspection and acceptance or rejection.

E.3 BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the TO and relevant terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

Acceptance will occur when all discrepancies, errors, or other deficiencies identified in writing by the Government have been resolved, through documentation updates, program correction, or other mutually agreeable methods.

Reports, documents, and narrative-type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected. If the deliverable is adequate, the Government may accept it or provide comments for incorporation.

All of the Government's comments on deliverables shall either be incorporated in the succeeding version of the deliverable, or the contractor shall explain to the Government's satisfaction why such comments should not be incorporated.

If the Government finds that a deliverable contains spelling errors, grammatical errors, or improper format, or otherwise does not conform to the quality assurance requirements stated within this TO, the document may be rejected without further review and returned to the contractor for correction and resubmission. If the contractor requires additional Government guidance to produce an acceptable version, the contractor shall arrange a meeting with the FEDSIM COR.

E.4 DELIVERABLES

The Government will provide written acceptance, comments, and/or change requests, if any, within 15 workdays (unless specified otherwise in Section F) from Government receipt of the deliverable. Upon receipt of the Government comments, the contractor shall have ten workdays to incorporate the Government's comments and/or change requests and to resubmit the deliverable.

E.5 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The FEDSIM CO or FEDSIM COR will provide written notification of acceptance or rejection (**Section J, Attachment H**) of all deliverables within 15 workdays (unless specified otherwise in **Section F**). All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

E.6 NON-CONFORMING PRODUCTS OR SERVICES

Non-conforming products or services will be rejected. Deficiencies shall be corrected, by the contractor, within ten workdays of the rejection notice. If the deficiencies cannot be corrected within ten workdays, the contractor shall immediately notify the FEDSIM COR of the reason for the delay and provide a proposed corrective action plan within ten workdays.

If the contractor does not provide products or services that conform to the requirements of this TO, the Government will document the issues associated with the non-conforming products or services in the Award Fee Determination Report, and there will be an associated impact to the potential award fee earned.

F.1 PERIOD OF PERFORMANCE

The period of performance for this TO is a one-year base period and four, one-year option periods:

Base Period:	March 9, 2021 – March 8, 2022
First Option Period:	March 9, 2022 – March 8, 2023
Second Option Period:	March 9, 2023 – March 8, 2024
Third Option Period:	March 9, 2024 – March 8, 2025
Fourth Option Period:	March 9, 2025 – March 8, 2026

F.2 PLACE OF PERFORMANCE

Most unclassified work shall be performed at a contractor facility. However, classified work shall be performed at the OUSD(C) in the NCR, contractor provided TS FCL facility, or another Government-approved and cleared facility. Additional places of performance may be indicated in each TDL.

CONUS and OCONUS travel is anticipated to be required in support of this effort.

F.3 TASK ORDER (TO) SCHEDULE AND MILESTONE DATES

The following schedule of milestones will be used by the FEDSIM COR to monitor timely progress under this TO.

The following abbreviations are used in this schedule:

DEL: Deliverable
IAW: In Accordance With
NLT: No Later Than
TOA: Task Order Award
All references to days: Calendar Days (unless stated otherwise)

Deliverables are due the next Government workday if the due date falls on a holiday or weekend.

Data Rights Clause - Abbreviations in the Gov't Rights column of the table below shall be interpreted as follows:

N/A: Not Applicable
UR: Unlimited/Unrestricted Rights, per Defense Federal Acquisition Regulation Supplement (DFARS) 252.227-7013 and 252.227-7014; and Unrestricted Rights, per DFARS 252.227-7015.

For software or documents that may be either proprietary COTS or custom, RS/LD rights apply to proprietary COTS software or documents and UR rights apply to custom software or documents. The Government asserts UR rights to open source COTS software. The contractor shall provide all applicable Supplier Agreements to the FEDSIM CO prior to purchase and cooperate with the Government in negotiating suitable terms to comply with Section H.13.1 and

H.13.2, which shall be "specific rights" pursuant to DFARS 227.7202-3. For purposes of the foregoing, the terms "Supplier Agreement" and "Commercial Supplier Agreement" have the same meaning.

The Government does not assert any rights to management software tools if the contractor does not plan to charge the Government directly for that tool and does not propose that the Government will own or use that tool.

The contractor shall deliver the deliverables listed in the following table on the dates specified:

DEL. #	MILESTONE/ DELIVERABLE	TO REFERENCE	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS
	Project Start (PS)		At TOA (NLT 10 days of TOA)	N/A
01	Project Kick-Off Meeting	C.5.1.2	Within 15 workdays of PS	N/A
02	Project Kick-Off Meeting Agenda	C.5.1.2	At least three workdays prior to the Kick-Off Meeting	UR – IAW DFARS 252.227-7013
03	Transition-In Plan	C.5.1.2 C.5.1.11	A draft transition plan is submitted with proposal. Upon award, the Government will provide comments. A final transition plan is due NLT 10 days after Government comment.	UR – IAW DFARS 252.227-7013
04	QMP	C.5.1.2 C.5.1.10	Due at Kick-Off Meeting; updated as changes in program processes are identified	UR – IAW DFARS 252.227-7013
05	EVM Plan	C.5.1.2 C.5.1.5	Due at Kick-Off Meeting; updated as changes in program processes are identified	UR – IAW DFARS 252.227-7013
06	Project Management Plan	C.5.1.2 C.5.1.3 C.5.1.7	10 days after receipt of Government comments	UR – IAW DFARS 252.227-7013
07	Project IMS	C.5.1.2 C.5.1.8	As Required	N/A

DEL. #	MILESTONE/ DELIVERABLE	TO REFERENCE	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS
08	Project Kick-Off Meeting Minutes Report	C.5.1.2	NLT five workdays of Kick-Off Meeting	UR – IAW DFARS 252.227-7013
09	TO Management Portal	C.5.1.3	Within 60 days of TOA, and as required when TO/TDL changes occur	UR – IAW DFARS 252.227-7013
10	Monthly Status Report (MSR)	C.5.1.3 C.5.1.4	Monthly, 15th calendar day of the next month	UR – IAW DFARS 252.227-7013
11	Technical Status Meeting	C.5.1.6	Monthly	UR – IAW DFARS 252.227-7013
12	Technical Status Meeting Minutes	C.5.1.6	Five workdays of Monthly Technical Status Meeting	UR – IAW DFARS 252.227-7013
13	Trip Report(s)	C.5.1.9	Within 10 days following completion of each trip	UR – IAW DFARS 252.227-7013
14	Transition-Out Plan	C.5.1.12	Within six months of PS; updates annually and then quarterly during the final Option Period	UR – IAW DFARS 252.227-7013
15	Finalized Written Products	F.5	Per TDL	UR – IAW DFARS 252.227-7013
16	PoR Transition Roadmap	C.5.1.13	Within three months of individual project completion	UR – IAW DFARS 252.227-7013
17	Future Products Process	C.5.2	As Required	UR – IAW DFARS 252.227-7013
18	Transition Planning	C.5.2.1	As Required	UR – IAW DFARS 252.227-7013
19	Lifecycle Management Process	C.5.2.5	As Required	UR – IAW DFARS 252.227-7013
20	DevSecOps Documentation	C.5.2.1	As Required	UR – IAW DFARS 252.227-7013
21	Weekly Status Report (WSR)	C.5.2.1.1	Weekly, every Monday or the next workday if Monday is a holiday	UR – IAW DFARS 252.227-7013

DEL. #	MILESTONE/ DELIVERABLE	TO REFERENCE	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS
22	Development Sprint Plan	C.5.2.1.1	As Required	UR – IAW DFARS 252.227-7013 and DFARS 252.227-7014
23	System Design Document (SDD)	C.5.2.1.1	As Required	UR – IAW DFARS 252.227-7013, 252.227-7014 and 252.227-7015
24	Database Design Document (DBDD)	C.5.2.1.1	As Required	UR – IAW DFARS 252.227-7013, 252.227-7014 and 252.227-7015
25	Test and Evaluation Master Plan (TEMP)	C.5.2.1.1	As Required	UR – IAW DFARS 252.227-7013
26	Bill of Materials (BOM)	C.5.2.1.1	As Required	UR – IAW DFARS 252.227-7013
27	User Training Plan	C.5.2.1.1	As Required	UR – IAW DFARS 252.227-7013
28	Release Plan	C.5.2.1.1	As Required	UR – IAW DFARS 252.227-7013
29	Requirements Traceability Matrix	C.5.2.1.1	As Required	UR – IAW DFARS 252.227-7013
30	Sprint Summary Report	C.5.2.1.1	As Required	UR – IAW DFARS 252.227-7013
31	System Migration Plan	C.5.2.2	As Required	UR – IAW DFARS 252.227-7013
32	Migration Procedures	C.5.2.2	As Required	UR – IAW DFARS 252.227-7013
33	Back-Out Procedures	C.5.2.2	As Required	UR – IAW DFARS 252.227-7013
34	Software Alternatives Information	C.5.2.3	As Required	UR – IAW DFARS 252.227-7013
35	Systems Solution Documentation	C.5.2.3	As Required	UR – IAW DFARS 252.227-7013
36	Total System Perspective	C.5.2.3	As Required	UR – IAW DFARS 252.227-7013

DEL. #	MILESTONE/ DELIVERABLE	TO REFERENCE	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS
37	Requirements Traceability and Change Impact Assessments	C.5.2.4	As Required	UR – IAW DFARS 252.227-7013
38	Test Plans	C.5.2.4	As Required	UR – IAW DFARS 252.227-7013
39	Final Test Report	C.5.2.4	As Required	UR – IAW DFARS 252.227-7013
40	Deficiencies Assessment	C.5.2.4	As Required	UR – IAW DFARS 252.227-7013
41	Test Procedure Improvements Recommendation	C.5.2.4	As Required	UR – IAW DFARS 252.227-7013
42	Trade-Off and Analysis of Alternatives Assessments	C.5.2.4	As Required	UR – IAW DFARS 252.227-7013
43	Cost Sharing Model	C.5.1.5	As Required	UR – IAW DFARS 252.227-7013
44	Service Catalog	C.5.4.1	As Required	UR-IAW DFARS 252-227-7014 and 252.227-7015
45	Memorandum of Agreements (MOA)	C.5.2.6.1	As Required	UR – IAW DFARS 252.227-7013
46	Monthly data quality issues	C.5.2.6.1	Monthly, 15th calendar day of the next month	UR – IAW DFARS 252.227-7013
47	Data Catalog	C.5.2.6.1	As Required	UR – IAW DFARS 252.227-7013
48	Application Program Interface (API) for data availability	C.5.2.6.1	As Required	UR – IAW DFARS 252.227-7013
49	Suite of Tools	C.5.2.6.1	As Required	UR – IAW DFARS 252.227-7013
50	CM Plan	C.5.2.6.2	As Required	UR – IAW DFARS 252.227-7013
51	Customer Outreach Plan	C.5.4.1	As Required	UR – IAW DFARS 252.227-7013

DEL. #	MILESTONE/ DELIVERABLE	TO REFERENCE	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS
52	Prototype and Design	C.5.5	As Required	UR – IAW DFARS 252.227-7013 252.227-7014
53	Community Feedback Process	C.5.4.1	As Required	UR – IAW DFARS 252.227-7013
54	Human Factors Interfaces Definitions	C.5.4.1	As Required	UR – IAW DFARS 252.227-7013
55	Innovation Results	C.5.5	As Required	UR – IAW DFARS 252.227-7013
56	Reserved			
57	Reserved			
58	Security Test Procedures	C.5.2.4	As Required	UR – IAW DFARS 252.227-7013 and DFARS 252.227-7014
59	Security Test Reports	C.5.2.4	As Required	UR – IAW DFARS 252.227-7013 and DFARS 252.227-7014
60	Secure API Definitions	C.5.3	As Required	UR – IAW DFARS 252.227-7013
61	Product PMP	C.5.4	As Required	UR – IAW DFARS 252.227-7013
62	Training Materials	C.5.4.1	As Required	UR – IAW DFARS 252.227-7013 and DFARS 252.227-7014
63	Reserved			
64	Reserved			
65	Reserved			
66	Reserved			
67	Access Management Process	C.5.4.1	As Required	UR – IAW DFARS 252.227-7013 and DFARS 252.227-7014
68	Event Monitoring Process	C.5.4.1	As Required	UR – IAW DFARS 252.227-7013 and DFARS 252.227-7014

DEL. #	MILESTONE/ DELIVERABLE	TO REFERENCE	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS
69	Request Fulfillment Process	C.5.4.1	As Required	UR – IAW DFARS 252.227-7013 and DFARS 252.227-7014
70	Incident Management Process	C.5.4.1	As Required	UR – IAW DFARS 252.227-7013 and DFARS 252.227-7014
71	Problem Management Process	C.5.4.1	As Required	UR – IAW DFARS 252.227-7013 and DFARS 252.227-7014
72	Quality Reports	C.5.4.1	As Required	UR – IAW DFARS 252.227-7013 and DFARS 252.227-7014
73	Monthly Customer Assistance Support activities	C.5.4.2	Monthly, 10th calendar day of the next month	UR – IAW DFARS 252.227-7013 and DFARS 252.227-7014
74	SOP Customer Assistance Support activities	C.5.4.2	As Required	UR – IAW DFARS 252.227-7013 and DFARS 252.227-7014
75	Monthly Customer Assistance Support metrics	C.5.4.2	Monthly, 10th calendar day of the next month	UR – IAW DFARS 252.227-7013
76	Emerging Technology Recommendations	C.5.5	As Required	UR – IAW DFARS 252.227-7013
77	Hardware/ Software Processes	C.5.5	As Required	UR – IAW DFARS 252.227-7013 and DFARS 252.227-7014
78	Copy of TO (initial award and all modifications)	F.4	Within 10 workdays of TOA, as required when TO changes occur	N/A
79	OPSEC SOP Plan	H.4	Within 90 calendar days of TOA	UR – IAW DFARS 252.227-7013

DEL. #	MILESTONE/ DELIVERABLE	TO REFERENCE	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS
80	Research Report Data Fusion PII and PHI Data	C.5.3	As Required	UR – IAW DFARS 252.227-7013 and DFARS 252.227-7014
81	Research Report Data Integration Environment	C.5.3	As Required	UR – IAW DFARS 252.227-7013 and DFARS 252.227-7014

The contractor shall mark all deliverables listed in the above table to indicate authorship by contractor (i.e., non-Government) personnel; provided, however, that no deliverable shall contain any proprietary markings inconsistent with the Government's data rights set forth in this TO. The Government reserves the right to treat non-conforming markings in accordance with DFARS 252.227-7013 and 252.227-7014.

F.4 PUBLIC RELEASE OF CONTRACT DOCUMENTS REQUIREMENT

The contractor agrees to submit, within ten workdays from the date of the FEDSIM CO's execution of the initial TO, or any modification to the TO (exclusive of Saturdays, Sundays, and Federal holidays), a Portable Document Format (PDF) file of the fully executed document with all proposed necessary redactions, including redactions of any trade secrets or any commercial or financial information that it believes to be privileged or confidential business information, for the purpose of public disclosure at the sole discretion of GSA (**Section F, Deliverable 78**). The contractor agrees to provide a detailed written statement specifying the basis for each of its proposed redactions, including the applicable exemption under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and, in the case of FOIA Exemption 4, 5 U.S.C. § 552(b)(4), shall explain why the information is considered to be a trade secret or commercial or financial information that is privileged or confidential. Information provided by the contractor in response to the contract requirement may itself be subject to disclosure under the FOIA. Submission of the proposed redactions constitutes concurrence of release under FOIA.

GSA will carefully consider the contractor's proposed redactions and associated grounds for nondisclosure prior to making a final determination as to what information in such executed documents may be properly withheld.

F.5 DELIVERABLES MEDIA

The contractor shall provide technical expertise, software, and hardware to ensure that deliverables, other data, or information related to work under **Section C.5** are converted into desired formats and stored electronically for easy dissemination among stakeholders. The end-product may be digital, physical copy, or both. The contractor shall provide technical writing and editing when necessary. The contractor shall also implement or develop professional style

guidelines and finalized written products when required by the task (**Section F, Deliverable 15**). Examples of this type of work would include formatting information into an electronic handbook, meeting the U.S. Government Printing Office (GPO) printing requirements, or compiling data into a hardcopy report suitable for distribution at a conference. Electronic documents shall be Microsoft (MS) Office compatible and able to be displayed on a Government computer workstation, using software generally available for Government use. The contractor shall curate document storage so information is stored logically and readily available to all appropriate stakeholders for efficient retrieval and use in research. Use of specialized software or hardware may be specified in associated TDLs.

The contractor shall deliver all electronic versions by electronic mail (email) and removable electronic media, as well as placing in the OUSD(C) designated repository. The contractor shall annually or as requested provide the FEDSIM COR with physical media that contains a copy of the TO Management Portal site content.

The following are the required electronic formats, whose versions must be compatible with the latest, commonly available version on the market.

a. Text	MS Word, Google Docs, PDF
b. Spreadsheets	MS Excel, Google Sheets
c. Briefings	MS PowerPoint, Google Slides
d. Drawings	MS Visio, Google Drawings
e. Schedules	MS Project, Smartsheet

F.6 PLACE(S) OF DELIVERY

Copies of all deliverables shall be delivered to the FEDSIM COR at the following address:

GSA Federal Acquisition Service (FAS) Assisted Acquisition Services (AAS) FEDSIM
ATTN: Brad Jordan, COR (QF0B)
1800 F Street, NW
Washington, D.C. 20405
Telephone: (202) 795-0907
Email: brad.jordan@gsa.gov

Copies of all deliverables shall also be delivered to the OUSD(C) TPOC.

F.7 NOTICE REGARDING LATE DELIVERY/PROBLEM NOTIFICATION REPORT (PNR)

The contractor shall notify the FEDSIM COR via a PNR (**Section J, Attachment E**) as soon as it becomes apparent to the contractor that a scheduled delivery will be late. The contractor shall include in the PNR the rationale for late delivery, the expected date for the delivery, and the project impact of the late delivery. The FEDSIM COR will review the new schedule and provide guidance to the contractor. Such notification in no way limits any Government contractual rights or remedies including, but not limited to, termination.

G.1 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The FEDSIM CO appointed a FEDSIM COR in writing through a COR Designation Letter (**Section J, Attachment A**). The FEDSIM COR will receive, for the Government, all work called for by the TO and will represent the FEDSIM CO in the technical phases of the work. The FEDSIM COR will provide no supervisory or instructional assistance to contractor personnel.

The FEDSIM COR is not authorized to change any of the terms and conditions, scope, schedule, and price of the Contract or the TO. Changes in the scope of work will be made only by the FEDSIM CO by properly executed modifications to the Contract or the TO.

G.1.1 CONTRACT ADMINISTRATION

Contracting Officer:

Kristen Jaremback
GSA FAS AAS FEDSIM (QF0B)
1800 F Street, NW
Washington, D.C. 20405
Telephone: 571-289-6715
Email: kristen.jaremback@gsa.gov

Contracting Officer's Representative:

Brad Jordan
GSA FAS AAS FEDSIM (QF0B)
1800 F Street, NW
Washington, D.C. 20405
Telephone: (703) 603-8116
Email: brad.jordan@gsa.gov

Technical Point of Contact:

Raymond Bombac (**Section J, Attachment P**)
OUSD(C)
Telephone: (703) 786-5397
Email: raymond.m.bombac.civ@mail.mil

G.2 INVOICE SUBMISSION

The contractor shall submit Requests for Payments in accordance with the format contained in General Services Acquisition Manual (GSAM) 552.232-25, PROMPT PAYMENT (NOV 2009), to be considered proper for payment. In addition, the following data elements shall be included on each invoice:

Task Order Number: *(from GSA Form 300, Block 2)*
Paying Number: *(ACT/DAC NO.) (From GSA Form 300, Block 4)*
FEDSIM Project Number: DE01101
Project Title: Technology Synchronization of Business Operations (TSyBO)

The contractor shall submit invoices as follows:

The contractor shall utilize FEDSIM's electronic Assisted Services Shared Information SysTem (ASSIST) to submit invoices. The contractor shall manually enter CLIN charges into Central Invoice Services (CIS) in the ASSIST Portal. Summary charges on invoices shall match the charges listed in CIS for all CLINs. The contractor shall submit invoices electronically by logging onto the following link (requires Internet Explorer to access the link):

https://portal.fas.gsa.gov

Log in using your assigned Identification (ID) and password, navigate to the order against which you want to invoice, click the Invoices and Acceptance Reports link in the left navigator, and then click the *Create New Invoice* button. By utilizing this method, no paper copy of the invoice shall be submitted to GSA FEDSIM or the GSA Finance Center. The contractor shall provide invoice backup data, as an attachment to the invoice, in accordance with the contract type, including detail such as labor categories, rates, and quantities of labor hours per labor category. The FEDSIM COR may require the contractor to submit a written "hardcopy" invoice with the client's certification prior to invoice payment. A paper copy of the invoice is required for a credit.

The contractor is certifying, by submission of an invoice in the CIS, that the invoice is correct and proper for payment.

If there are any issues submitting an invoice, contact the Assisted Acquisition Services Business Systems (AASBS) Help Desk for support at 877-472-4877 (toll free) or by email at AASBS.helpdesk@gsa.gov.

G.3 INVOICE REQUIREMENTS

The contractor shall submit a draft copy of an invoice backup in Excel to the FEDSIM COR and OUSD(C) TPOC for review prior to its submission to ASSIST. The draft invoice shall not be construed as a proper invoice in accordance with FAR 32.9 and GSAM 532.9. The contractor shall provide receipts on an as-requested basis.

Each contract type shall be addressed separately in the invoice submission.

The final invoice is desired to be submitted within six months of project completion. Upon project completion, the contractor shall provide a final invoice status update monthly.

Regardless of contract type, the contractor shall report the following data:

a. Government Wide Acquisition Contract (GWAC) Number.
b. TOA Number (NOT the Solicitation Number).
c. Contractor Invoice Number.
d. Contractor Name.
e. POC Information.
f. Current period of performance.
g. Amount of invoice that was subcontracted.

The amount of invoice that was subcontracted to a small business shall be made available upon request.

G.3.1 COST-PLUS-AWARD-FEE (CPAF) CLINs (for LABOR)

The contractor may invoice monthly on the basis of cost incurred for the CPAF CLINs. The invoice shall include the period of performance covered by the invoice (all current charges shall be within the active period of performance) and the CLIN number and title. All hours and costs shall be reported by CLIN element (as shown in Section B), by contractor employee, and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

a. Employee name (current and past employees).
b. Employee company.
c. Exempt or non-exempt designation.
d. Employee Alliant 2 labor category.
e. Current monthly and total cumulative hours worked.
f. Direct Labor Rate.
g. Effective hourly rate (e.g., cumulative costs/cumulative hours).
h. Current approved billing rate percentages in support of costs billed.
i. Itemization of cost centers applied to each individual invoiced.
j. Itemized breakout of indirect costs (e.g., Fringe, Overhead (OH), General and Administrative (G&A) burdened costs for each individual invoiced (rollups are unacceptable)).
k. Any cost incurred not billed by CLIN (e.g., lagging costs).
l. Labor adjustments from any previous months (e.g., timesheet corrections).
m. Provide comments for deviation outside of ten percent of estimates and/or expected values.
n. Funding and cost incurred by TDL.

All cost presentations provided by the contractor in Excel shall show indirect charges itemized by individual with corresponding indirect rates with cost center information. The invoice detail shall be organized by CLIN.

The contractor may invoice for fee after accepting the modification which includes the award fee determination and any corresponding deobligation of unearned fee. See the AFDP in **Section J, Attachment D** for additional information on the award fee determination process.

When the Incurred Cost method is used to determine the Award Fee Pool Allocation for an Award Fee period, the incurred cost shall be calculated using approved provisional billing rates as established by the cognizant Government auditor, in accordance with FAR 42.704. Approved provisional billing rates shall not be adjusted for the purpose of accumulating incurred costs and calculating the Award Fee Pool Allocation.

G.3.2 TOOLS AND OTHER DIRECT COSTS (ODCs)

The contractor may invoice monthly on the basis of cost incurred for the Tools and ODC CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. In addition, the contractor shall provide the following detailed information for each invoice submitted, as applicable. Spreadsheet submissions are required.

a. Tools and/or ODCs purchased.
b. RIP or CTP number or identifier.
c. Date accepted by the Government.
d. Associated CLIN.
e. Project-to-date totals by CLIN.
f. Cost incurred not billed by CLIN.
g. Remaining balance of the CLIN.
h. Any applicable Fee.

All cost presentations provided by the contractor shall also include any indirect costs being applied with associated cost center information.

G.3.3 TRAVEL

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

a. Federal Travel Regulation (FTR) - prescribed by the GSA, for travel in the continental United States (U.S.).
b. Joint Travel Regulations (JTR) Volume 2, DoD Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.
c. Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, “Maximum Travel Per Diem Allowances for Foreign Areas” - prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

The contractor may invoice monthly on the basis of cost incurred for cost of travel comparable with the JTR/FTR/DSSR. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. Separate worksheets, in MS Excel format, shall be submitted for travel.

CLIN Total Travel: This invoice information shall identify all cumulative travel costs billed by CLIN. The current invoice period’s travel details shall include separate columns and totals and include the following:

a. TAR number or identifier, approver name, and approval date.
b. Current invoice period.
c. Names of persons traveling.
d. Number of travel days.
e. Dates of travel.
f. Number of days per diem charged.

g. Per diem rate used.
h. Total per diem charged.
i. Transportation costs.
j. Total charges.
k. Explanation of variances exceeding ten percent of the approved versus actual costs.
l. Indirect handling rate.
m. Funding and cost incurred by TDL.

All cost presentations provided by the contractor shall also include OH charges and G&A charges in accordance with the contractor's Defense Contract Audit Agency (DCAA) cost disclosure statement.

G.4 TASK ORDER (TO) CLOSEOUT

The Government will unilaterally close out the TO no later than six years after the end of the TO period of performance if the contractor does not provide final DCAA rates by that time.

H.1 KEY PERSONNEL

The following are the minimum personnel who shall be designated as "Key." The Government does not intend to dictate the composition of the ideal team to perform this TO.

a. Program Manager (PM)
b. Enterprise Architecture (EA) Engineering Lead
c. System Engineering (SE) Lead
d. Information Assurance (IA) Engineer

All required and desired qualifications shall be applicable at the time of proposal submission. The Government desires that Key Personnel be assigned for the duration of the TO.

H.1.1 PROGRAM MANAGER (PM)

The contractor shall identify a PM by name who shall provide management, direction, administration, quality assurance (as defined in **Section C.5.1**), and leadership of the execution of this TO. The PM shall act as the overall lead, manager, and administrator for the effort. The PM shall direct efforts of cross-competency teams, including contractors at multiple locations, and serve as the primary interface and POC with Government program authorities and representatives on technical and project issues. The PM shall be responsible for regularly briefing leadership on program status and milestones. The PM shall oversee contractor personnel project operations by developing procedures; planning and directing execution of the contractual, technical, multi-disciplinary engineering, programming, maintenance, and administrative support effort; and monitoring and reporting progress. The PM shall manage acquisition and employment of project resources and control financial and administrative aspects of the project.

It is required that the PM has the following qualifications:

a. Possess a minimum of an active Top Secret (TS) security clearance with Sensitive Compartmented Information (SCI) eligibility.
b. Be an employee of the prime offeror or have an offer of employment from the prime offeror that the Key Person intends to accept in the event of an award being made to the offeror.
c. Possess a minimum of ten years of Project Management experience managing complex projects in an IT engineering or big data environment similar to Section C requirements.
d. Possess an active certification in one of the following:
    1. Project Management Institute (PMI) Project Management Professional, PMI Program Management Professional (PgMP) certification, or equivalent program or project management certification.
    2. Federal Acquisition Certification for Program and Project Managers (FAC P/PM) Level 3.
    3. Defense Acquisition Workforce Improvement Act (DAWIA) Level III Program Management certification.
e. Possess a minimum of five years of experience managing projects utilizing non-traditional program management methodologies (e.g., Agile) in a big data environment.

f. Possess a minimum of five years of experience in a military or other Government environment performing in a related subject area (e.g., project management, engineering, or computer science) to that of this TO.

It is desired that the PM has the following qualification:

a. Possess a Master of Business and Management (MBM), a Master of Business Administration (MBA), or a master's degree in a related technical discipline (e.g., Engineering, Computer Science, or Electronics).

H.1.2 EA ENGINEERING LEAD

The EA Engineering Lead shall act as the lead for architecting, positioning, designing, developing, and deploying solutions, including the oversight of all integration efforts into their intended systems and subsystems. The EA Engineering Lead shall direct the efforts of all product line teams at multiple locations and serve as the primary interface and POC for all EA-related issues. The EA Engineering Lead shall ensure that any technologies incorporated into or developed under this TO do not conflict with the program baseline. The EA Engineering Lead shall also ensure the most advanced technology vendors are engaged in the process and the program has reach across industry to engage the best solutions.

It is required that the EA Engineering Lead has the following qualifications:

a. Possess a minimum of an active TS security clearance with SCI eligibility.
b. Possess a minimum of five years of experience with data modeling, data engineering, feature engineering, data access, application development, model lifecycle management, and cloud infrastructure.
c. Possess a minimum of five years of experience with the Software Development Lifecycle (SDLC) and agile software development practices.
d. Possess a minimum of five years of experience with data visualization packages in Python or similar programming languages.
e. Possess a minimum of five years of experience engaging multiple stakeholders from industry to rapidly advance software development.

It is desired that the EA Engineering Lead has the following qualifications:

a. Possess a minimum of five years of experience with supervised and unsupervised deep learning algorithms like Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Gated Recurrent Unit (GRU) and advanced deep learning packages such as TensorFlow, Keras, Pytorch, Caffe, and Theano.
b. Possess a minimum of five years of developmental experience highlighting proficiency in meaningful programming languages (e.g., Go, Python, Java, Scala, C++).
c. Possess a minimum of five years of experience in an IC, military, or other Government environment performing in a capacity related to the EA Engineering Lead role.

H.1.3 SE LEAD

The SE Lead shall work in conjunction with the EA Engineering Lead and be responsible for leading the cloud systems plans and strategy, developing and deploying applications into a Cloud

or Hybrid Cloud, and implementing enterprise infrastructure and platforms required for cloud computing. The SE Lead's responsibilities shall include leading the development and integration of cloud-based information and computer systems that meet specific needs, as identified in the TO. The SE Lead shall also be accountable for the end-to-end cloud deployment experience, from concept development to deployment.

It is required that the SE Lead has the following qualifications:

a. Possess a minimum of an active TS security clearance with SCI eligibility.
b. A minimum of ten years of experience supporting architecture design, development, implementation, and maintenance.
c. A minimum of one of the following professional certifications:
    1. Professional Cloud Solutions Architect (PCSA).
    2. Amazon Web Services (AWS) Solutions Architect (Professional).
    3. MS Certified Azure Solutions Architect (Expert).
    4. Google Cloud Certified Architect (Professional).

It is desired that the SE Lead has the following qualifications:

a. Experience with one of the large cloud-computing infrastructure solutions similar to AWS, MS Azure, or Google Cloud Platform (GCP) environment.
b. Experience supporting highly distributed applications.
c. Experience leading a cross-functional technology team.
d. Possess one of the following AWS Certifications:
    1. AWS Certified SysOps Administrator (Associate).
    2. AWS Certified DevOps Engineer (Professional).
    3. AWS Certified Big Data (Specialty).
e. Experience utilizing Agile development methodologies and Application Lifecycle Management.
f. Experience working with programming languages such as Java, C++, JSON, PHP, Perl, Python, Ruby, Pig/Hive, and/or Elixir.

H.1.4 IA ENGINEER

The IA Engineer shall serve as the senior POC and lead for ensuring that Government and industry best practices for maintaining Confidentiality, Integrity, and Availability (CIA) of IT systems and services are applied and executed for the IT EA services.

It is required that the IA Engineer has the following qualifications:

a. Current Certified Information Systems Security Professional (CISSP).
b. Possess a minimum of an active TS security clearance with SCI eligibility.
c. Possess a minimum of five years of experience applying DoD Security Management and Security Engineering policy guidance and directives to both hardware and software-centric environments.
d. Possess a minimum of five years of experience with DoD RMF, vulnerability assessments, IA Vulnerability Alerts (IAVA) reporting, and IA problem resolution.

It is desired that the IA Engineer has the following qualifications:

a. At least five years of experience with applying security principles and best practices in a development environment.
b. At least five years of experience with current and emerging IA enterprise security practices.
c. At least five years of experience with developing, testing, and sustaining a secure solution in a changing environment.
d. At least five years of experience managing a team responsible for developing and implementing enterprise security policies and practices.

H.1.4 KEY PERSONNEL SUBSTITUTION

The contractor shall not replace any personnel designated as Key Personnel without the written concurrence of the FEDSIM CO. Prior to utilizing other than the Key Personnel specified in its proposal in response to the TOR, the contractor shall notify the FEDSIM CO and the FEDSIM COR. This notification shall be no later than ten calendar days in advance of any proposed substitution and shall include justification (including resume(s) and labor category of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on TO performance.

Substitute Key Personnel qualifications shall be equal to, or greater than, those of the Key Personnel substituted. If the FEDSIM CO and the FEDSIM COR determine that a proposed substitute Key Personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the contractor may be subject to default action as prescribed by FAR 52.249-6 Termination.

H.2 GOVERNMENT-FURNISHED PROPERTY (GFP)

The Government will provide access to facilities, office space, supplies, and services including workstations, computers, connectivity, and telephones for contractor personnel providing on-site support. Access will be granted to classified and unclassified Local Area Network (LAN) services, LAN support, telephones, and reproduction facilities. Other than access to facilities and meeting space, as needed, the Government will not provide any GFP to contractor personnel providing off-site support.

If the contractor determines additional equipment is required, the contractor shall notify the FEDSIM COR and OUSD(C) TPOCs, in writing, of the applicable equipment required to accomplish the requirements.

The contractor shall be held accountable for the loss or destruction of Government property in the custody of contractor personnel, as documented and acknowledged in accordance with OUSD(C) policies and regulations.

H.3 GOVERNMENT-FURNISHED INFORMATION (GFI)

The Government will provide access to relevant Government organizations, information, documentation, manuals, text briefs, and associated materials, as required and available.

The Government will provide all information necessary for completion of the requirements after TOA. The contractor shall use GFI, Government-furnished data, and Government-furnished

documents only for the performance of work under this TO. The contractor shall be responsible for returning all GFI, Government-furnished data, and Government-furnished documents to the Government at the end of the performance period. The contractor shall not release GFI, Government-furnished data, and Government-furnished documents to outside parties without the prior and explicit consent of the FEDSIM CO.

H.4 SECURITY REQUIREMENTS

All references to the contractor and/or contractor personnel include all members of the contractor team including, but not limited to, any subcontractors or teaming partners.

The contractor shall comply with all applicable security requirements, directives, instructions, and SOPs. The contractor shall follow all security policies, procedures, and requirements stipulated in the National Industrial Security Program (NISP), National Industrial Security Program Operating Manual (NISPOM), and any supplements thereto, including applicable FAR and DFARS guidelines/requirements.

All classified systems and personnel security must be in accordance with the NISPOM. Contractor personnel performing IT-sensitive duties are subject to investigative and assignment requirements in accordance with IA, personnel security, and other affiliated regulations. Additional Operations Security (OPSEC) requirements to the NISPOM are in effect, and the Government will provide its OPSEC Plan to the contractor. The contractor shall develop an OPSEC SOP Plan (**Section F, Deliverable 79**) within 90 calendar days of TOA and submit it to the FEDSIM COR and OUSD(C) TPOC/OPSEC officer to be reviewed and approved per DoD regulations. This OPSEC SOP Plan shall include the Government's critical information, why it needs to be protected, where it is located, who is responsible for it, and how to protect it. The contractor shall implement its OPSEC SOP Plan upon approval by the Government. In addition, the contractor shall identify an individual who will be an OPSEC Coordinator. Within 90 days of PS, the contractor shall ensure the individual becomes OPSEC Level II certified.

The contractor shall be required to have access to all applicable program/project Security Classification Guides (SCG), the IT Enterprise (ITE), the National Security Agency intranet (NSANet), the Secret Internet Protocol Router Network (SIPRNet), and the Non-classified Internet Protocol Router Network (NIPRNet) as applicable to the systems being supported.

H.4.1 INFORMATION ASSURANCE

The contractor may have access to sensitive (including privileged and confidential) data, information, and materials of the U.S. Government (USG). These printed and electronic documents are for internal use only and remain the sole property of the USG. Some of these materials are protected by the Privacy Act of 1974 (AMENDED) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.

Performance under the TO may require the contractor to access data and information sensitive to another Government agency, another Government contractor, or of such nature that its dissemination or use other than as specified in this TO would be averse to the interests of the Government or others. Neither the contractor, nor its contractor personnel, shall divulge or release any information developed or obtained in the course of TO performance, except to specifically authorized Government personnel, or upon written approval of the FEDSIM CO.

The contractor shall not use, disclose, or reproduce any sensitive contract information that bears a restrictive legend, other than as specified in this TO.

H.4.2 CLASSIFICATION

The association between the contractor and the Government is unclassified; however, disclosure of TO specifics is on a need-to-know basis. The Government anticipates work under this TO will be conducted at multiple security levels. Work under this TO may be classified up to TS/SCI.

H.4.3 PUBLIC KEY INFRASTRUCTURE (PKI) REQUIREMENTS

Where interoperable, DoD PKI or CACs are required for the exchange of unclassified information between DoD and contractors or for access to Public Key-enabled information systems and websites. Contractors shall obtain all necessary certificates. The Government will support the issuing of CACs.

The contractor shall provide the appropriate documentation to the Government in order to be properly provided with the Government CAC. The contractor shall comply with all DoD regulations concerning the acquisition of CACs for all contractor personnel, in accordance with the policies and procedures currently in use at each Government location.

H.4.4 SECURITY CLEARANCES

Contractor personnel (including subcontractors, if proposed) under this TO are required to have the appropriate level of personnel security clearance before performing any work under this TO. Some positions and functional roles may not require a security clearance as stated in DD 254, and other tasks may require an active clearance level up to TS clearance with an SCI determination reflected in Joint Personnel Adjudication System (JPAS) or Scattered Castles.

All Cyber Security Engineers, ISSO/Privacy Engineers, and System Engineers that support Backend Operations must have a minimum of a TS security clearance with SCI and Counterintelligence (CI) Scope Polygraph eligibility at project start.

All contractor personnel with access to a Government accredited Sensitive Compartmented Information Facility (SCIF) at either Government or contractor facilities shall hold the appropriate clearances for the work to be performed.

Contractor personnel that require a security clearance shall have undergone a Single Scope Background Investigation (SSBI) or an SSBI Periodic Review (SSBI-PR) within the last six years that was favorably adjudicated. If the SSBI-PR is overdue as a result of Government delays in processing background investigations, the contractor personnel shall continue to be eligible for access to classified information if the current eligibility is indicated in JPAS. The exception to the preceding sentence is if the Government is aware of relevant derogatory information related to an individual's continued eligibility for access, then the contractor personnel may be denied access. All contractor personnel that require access to SCI information shall be formally nominated by their company's security office to be indoctrinated into SCI programs. Additionally, the contractor personnel supporting a Special Access Program (SAP) shall be required to successfully complete a CI Scope Polygraph in accordance with IC Policy Guidance 704.6 and DoD Directive (DoDD) 5210.48 or have a valid polygraph examination displayed in JPAS or Scattered Castles from another Federal agency to be reviewed to determine reciprocity.

If any contractor personnel are unable to obtain a TS clearance with access to SCI within 30 calendar days of initiating support under this TO, except as noted above with Government approval by the OUSD(C) TPOC and FEDSIM CO, the contractor shall:

a. Notify the Government (i.e., OUSD(C) TPOC and FEDSIM CO).
b. Terminate billing for the employee against the TO.

Furthermore, if any personnel employed by the contractor in support of this TO fail to maintain the required security clearance or access, the contractor shall:

a. Notify the OUSD(C) TPOC and FEDSIM CO of this discrepancy.
b. Remove the employee from the USG Program Office designated site.
c. Terminate billing for the employee against the TO effective the date of loss of clearance.

The contractor shall ensure all security, misconduct, or performance-related incidents are reported to the FEDSIM COR and the contractor's Facility Security Officer (FSO) immediately upon discovery of the incident. Once reported to the FEDSIM COR and the FSO and within seven working days of the incident, the contractor's FSO shall report the incident in JPAS. Incidents that are not reported in the time frame and manner prescribed above may result in the incident along with the contractor's FSO being reported to the Defense Security Service (DSS) as a security violation and/or TO performance failure.

The contractor shall plan for attrition through careful scheduling and advance preparation and submission of clearance requests. A sufficient number of relief personnel to cover absenteeism and special events shall be cleared to ensure quality service. The Government (i.e., OUSD(C)TPOC and FEDSIM CO) will pre-approve all personnel submitted for a clearance.

Contractor personnel shall wear the Government-provided ID badge at all times when performing work under this TO, including attending Government meetings and conferences within the facility. The contractor shall wear the ID badge in a conspicuous place on the front of exterior clothing and above the waist except when safety or health reasons prohibit such placement.

Contractor personnel who do not hold valid security clearances to Government facilities shall coordinate their visits in advance with the FEDSIM COR, OUSD(C) TPOC, or Government POC. Final approval for facility access must be granted by the OUSD(C) TPOC before arrival at the designated location.

The Government will provide appropriate SCGs and additional instructions within the DD Form 254 (**Section J, Attachment J**). In general, all necessary facility and employee security clearances shall be at the expense of the contractor. The contractor shall comply with all security requirements.

H.4.5 FACILITY CLEARANCE LEVEL (FCL)

The contractor shall adhere to and comply with the security guidelines and requirements outlined in the Department of Defense (DD) Form 254 (**Section J, Attachment J**), which requires the contractor to possess a TS FCL. The Government will provide appropriate SCGs and additional instructions within the DD Form 254. The contractor shall follow instructions for public release requirements and disclosure policy references in the DD Form 254 Contract Security

Classification Specification Block 12 as well as additional security guidance and requirements in Blocks 13 and 14.

H.4.6 FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE (FOCI)

The contractor shall comply with the FOCI evaluation and mitigation process in accordance with the NISPOM, DoD 5220.22-M, Chapter 2, Section 3 (Incorporating Change 2, May 18, 2016). As such:

a. The contractor and any subcontractors shall be FOCI active with the OUSD(C) to be eligible to work on the TO.
b. The mission sponsor will associate FOCI eligibility with the business unit's Taxpayer Identification Number (TIN) as submitted to start work on the TO.

H.4.7 SAFEGUARDING SENSITIVE DATA AND IT RESOURCES

H.4.7.1 GENERAL REQUIREMENTS FOR PII/PHI

This Section addresses the contractor's requirements under The Privacy Act of 1974 (Privacy Act), The Freedom of Information Act (FOIA), and The Health Insurance Portability and Accountability Act (HIPAA) as set forth in applicable statutes, implementing regulations and Department of Defense (DoD) issuances. In general, the contractor shall comply with the specific requirements set forth in this Section and elsewhere in this TO. The contractor shall also comply with requirements relating to records management as described herein.

This TO incorporates by reference the federal regulations and DoD issuances referred to in this Section. If any authority is amended or replaced, the changed requirement is effective when it is incorporated under contract change procedures. Where a federal regulation and any DoD issuance govern the same subject matter, the contractor shall first follow the more specific DoD implementation unless the DoD issuance does not address or is unclear on that matter. DoD issuances are available at http://www.dtic.mil/whs/directives.

For purposes of this Section, the following definitions apply.

DoD Privacy Act Issuances means the DoD issuances implementing the Privacy Act, which are Department of Defense Instruction (DoDI) 5400.11, DoD Privacy and Civil Liberties Programs, January 29, 2019 and DoDI 5400.11-R, Department of Defense Privacy Program, May 14, 2007.

HIPAA Rules means, collectively, the HIPAA Privacy, Security, Breach and Enforcement Rules, issued by the U.S. Department of Health and Human Services (HHS) and codified at 45 Code of Federal Regulations (CFR) Part 160 and Part 164, Subpart E (Privacy), Subpart C (Security), Subpart D (Breach) and Part 160, Subparts C-E (Enforcement), as amended. Additional HIPAA rules regarding electronic transactions and code sets (45 CFR Part 162) are not addressed in this Section and are not included in the term HIPAA Rules.

DoD HIPAA Issuances means the DoD issuances implementing the HIPAA Rules in the DoD Military Health System (MHS). These issuances are Department of Defense Manual (DoDM) 6025.18, "Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs," March 13, 2019, DoDI 6025.18 Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care

Programs, March 13, 2019, and DoDI 8580.02, Security of Individually Identifiable Health Information in DoD Health Care Programs, August 12, 2015.

Defense Health Agency (DHA) Privacy Office is the DHA Privacy and Civil Liberties Office. The DHA Privacy Office Chief is the HIPAA Privacy and Security Officer for DHA.

H.4.7.2 PII/PHI DATA

The contractor shall not use or further disclose PII / PHI other than as permitted or required by the TO or as Required by Law.

The contractor shall use appropriate safeguards and comply with the HIPAA Security Rule with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for by the TO.

The contractor shall report to OUSD(C) any breach of which it becomes aware and shall proceed with breach response steps as required. With respect to electronic PHI, the contractor shall also respond to any security incident of which it becomes aware in accordance with any applicable DoD cybersecurity and National Institute of Standards and Technology (NIST) requirements. If at any point the contractor becomes aware that a security incident involves a breach, the contractor shall immediately initiate breach response as required by this Section.

In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), respectively, as applicable, the contractor shall ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the contractor agree to the same restrictions, conditions, and requirements that apply to the contractor with respect to such PHI.

With respect to individual rights of access to PHI, the contractor shall make available PHI in a designated record set to the individual or the individual's designee as necessary to satisfy DoD's obligations under the DoD HIPAA Issuances and the corresponding 45 CFR 164.524. If the contractor intends to deny the individual's request, the contractor shall forward it (within seven working days of receipt) to the DHA Privacy Office. The DHA Privacy Office shall make a determination within 20 calendar days (50 calendar days for justified delays) of the request. The DHA Privacy Office shall notify the individual, with a copy to the contractor, of any approved or denied access determinations and the reason for any denial. The individual may appeal the denial determination to the DHA Privacy Office.

The contractor shall make any amendment(s) to PHI in a designated record set as directed or agreed to by OUSD(C) or take other measures as necessary to satisfy DoD's obligations under the DoD HIPAA Issuances and the corresponding 45 CFR 164.526.

The contractor shall maintain and make available to the Government the information required to provide an accounting of disclosures to the OUSD(C) or to the individual as necessary to satisfy DoD's obligations under the DoD HIPAA Issuances and the corresponding 45 CFR 164.528.

H.4.7.3 RECORDS MANAGEMENT

When creating and maintaining official Government records, the contractor shall comply with all federal requirements established by 44 United States Code (U.S.C.) Chapters 21, 29, 31, 33 and 35, and by 36 CFR, Chapter XII, Subchapter B – Records Management. The contractor shall also comply with DoD Administrative Instruction No. 15 (DoD AI-15), "OSD Records and

Information Management Program" (May 3, 2013) and Records Management requirements outlined in the current TRICARE Operations Manual (TOM).

H.4.7.4 FREEDOM OF INFORMATION ACT (FOIA)

The contractor shall comply with the following procedures if it receives a FOIA request and immediately contact the DHA FOIA Officer for evaluation/action:

The contractor shall inform beneficiaries that DHA FOIA procedures require a written request preferably sent via the National FOIA Portal at: www.FOIA.gov. However, requestors may also submit requests via email at DHA.FOIA@mail.mil; or via postal delivery addressed to the DHA Freedom of Information Service Center, 7700 Arlington Boulevard, Suite 5101, Falls Church, Virginia 22042-5101. All FOIA requests shall describe the desired record as completely as possible to facilitate its retrieval from files and to reduce search fees which may be borne by the requestor. TO and/or Modification numbers must be included in all FOIA requests seeking DHA procurement records. Although the administrative time limit to grant or deny a request (ten working days after receipt) does not begin until the request is received by DHA, the contractor shall act as quickly as possible and respond to DHA within ten working days.

In response to requests received by the contractor for the release of information, unclassified information, documents and forms which were previously provided to the public as part of routine services shall continue to be made available in accordance with previously established criteria. All other requests from the public for release of DHA records and, specifically, all requests that reference FOIA shall be immediately forwarded to DHA, ATTENTION: Freedom of Information Officer, for appropriate action. Direct contact, including interim replies, between TRICARE contractors and such requestors is not authorized. The contractor shall process requests by individuals for access to records about themselves in accordance with directions from the DHA Freedom of Information Service Center. If such a requestor specifically makes the request under the Privacy Act or does not make clear whether the request is made under FOIA or the Privacy Act, the contractor shall process the request in accordance with directions from the DHA Privacy Office. If requestor specifically seeks PHI under HIPAA, the contractor shall follow Section H.3.5.8, relating to individual rights of access to PHI.

H.4.7.5 PRIVACY IMPACT ASSESSMENT (PIA)

DHA data will not be stored on a contractor owned system with this TO, so PIA is not required from the contractor.

H.4.7.6 DATA SHARING AGREEMENT (DSA)

H.4.7.6.1 DHA DATA

A DSA applies if TO requirements involve the use of DHA data (including PII/PHI, a limited data set, or de-identified data).

The contractor shall consult with the DHA Privacy Office to determine if the contractor must obtain a DSA or Data Use Agreement (DUA), when DHA data will be accessed, used, disclosed or stored, to perform the requirements of this TO.

The contractor shall comply with the permitted uses established in a DSA/DUA to prevent the unauthorized use and/or disclosure of any PII/PHI, in accordance with the HIPAA Rules and DoD HIPAA Issuances. Likewise, the contractor shall comply with the DoD Privacy Act Issuances.

Prior to using any data involving PHI for research purposes, as defined by HIPAA, the contractor shall gain approval from the DHA Privacy Board. Thus, the contractor shall comply with DHA Privacy Board requests for additional documentation.

To begin the DSA request process, the contractor shall submit a DSA Application (DSAA) to the DHA Privacy Office. Upon approval, the requestor shall enter into one of the following agreements, depending on the data involved:

a. DSA for De-Identified Data
b. DSA for PHI
c. DSA for PII Without PHI
d. DUA for Limited Data Set

DSAs executed for TO support will expire after one year or at the end of the TO order period, whichever comes first. If the contractual use of DHA data will continue after the DSA expiration date, the contractor shall submit a DSA Renewal Request template to the Privacy Office; however, if the DSA will not be renewed, the contractor shall close the DSA by providing a Certificate of Data Disposition (CDD) to the DHA Privacy Office.

H.4.7.6.2 HUMAN SUBJECT RESEARCH

This TO incorporates by reference the Protection of Human Subject Research clause in the Defense Federal Acquisition Regulation Supplement (DFARS) at 48 CFR 252.235-7004. A separate DFARS provision, 48 CFR 235.072(e), requires that the clause be incorporated in contracts that include or may include research involving human subjects in accordance with 32 CFR 219, DoDI 3216.02, and 10 U.S.C. 980, including research that meets exemption criteria under 32 CFR 219.101(b), the clause applies to solicitations and contracts awarded involving any DoD component, regardless of mission or funding Program Element Code. Thus, in the event a contractor participates in a study or demonstration project or other activity that involves human subject research, then the contractor shall comply with Protection of Human Subject Research clause. COs may not determine whether an activity is exempt from human subject research requirements. If contractor activity appears to involve human subject research, then the contractor shall consult the DHA Privacy Office, which may contact the Research Regulatory Oversight Office in the Office of the Under Secretary of Defense for Personnel and Readiness (OUSD(P&R)).

H.4.7.7 PRIVACY ACT AND HIPAA TRAINING

The contractor shall ensure that its entire staff, including subcontractors and consultants that perform work on this TO receive training on the Privacy Act, HIPAA, and the federal regulations on confidentiality of substance use disorder patient records, 42 CFR Part 2. Refer to FAR 52.224-3 regarding specific requirements for Privacy Training appropriate to the contractor's scope of involvement with DHA's PHI and its regulatory responsibilities as either

a Covered Entity, or Business Associate.

The contractor shall ensure all employees and subcontractors supply a certificate of all training completion to the FEDSIM COR within 30 days of being assigned.

H.4.7.8 HIPAA BUSINESS ASSOCIATE PROVISIONS

The contractor meets the definition of Business Associate, and DHA meets the definition of a covered entity under the HIPAA Rules and the DoD HIPAA Issuances. Therefore, a Business Associate Agreement (BAA) between the contractor and DHA is required to comply with the HIPAA Rules and the DoD HIPAA Issuances. The contractor shall use the DoD BAA, which shall be used by all organizational entities within the DoD, referred to collectively as the "DoD Components", located at https://www.health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Privacy-Contract-Language/HIPAA-Compliant-Business-Associate-Agreement-for-theMHS. b.i and (3)b.ii.

H.4.7.9 BREACH RESPONSE

H.4.7.9.1 DEFINITIONS RELATED TO BREACH RESPONSE

Breach means a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than an authorized purpose have access or potential access to PII, whether physical or electronic. The foregoing definition is based on the definition of breach in DoDD 5400.11. Breaches are classified as either possible or confirmed (see the following two definitions) and as either cyber or non-cyber (i.e., involving either electronic PII/PHI or paper/oral PII/PHI).

A possible breach is an incident where the possibility of unauthorized access is suspected (or should be suspected) and has not been ruled out. For example, if a laptop containing PII/PHI is lost, and the contractor does not initially know whether or not the PII/PHI was encrypted, the incident must initially be classified as a possible breach because it is impossible to rule out the possibility of unauthorized access to the PII/PHI.

In contrast, when misdirected postal mail is returned unopened in its original packaging, a possible breach has not occurred and the possibility can be ruled out immediately. However, if the intended recipient informs the contractor that an expected package has not been received, then a possible breach exists until and unless the unopened package is returned to the contractor. In determining whether unauthorized access should be suspected, the contractor shall consider at least the following factors:

a. How the event was discovered?
b. Did the information stay within the covered entity's control?
c. Was the information actually accessed/viewed?
d. Ability to ensure containment (e.g., recovered, destroyed, or deleted).

A confirmed breach is an incident in which it is known that unauthorized access could occur. For example, if a laptop containing PII/PHI is lost and the contractor knows that the PII/PHI is unencrypted, then the contractor should classify and report the incident as a confirmed breach,

because unauthorized access could occur due to the lack of encryption (the contractor knows this even without knowing whether or not unauthorized access to the PII/PHI has actually occurred). If the laptop is subsequently recovered and forensic investigation reveals that files containing PII/PHI were never accessed, then the possibility of unauthorized access can be ruled out, and the contractor should re-classify the incident as a non-breach incident.

A HHS breach is an incident that satisfies the definition of breach in Section 164.402 of the HIPAA Breach Rule. The text of the HHS definition states: *Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E of this part [i.e. the HIPAA Privacy Rule] which compromises the security or privacy of the PHI.*

HHS breach excludes:

i. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a DoD covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule.
ii. Any inadvertent disclosure by a person who is authorized to access PHI at a DoD covered entity or business associate to another person authorized to access PHI at the same DoD covered entity or business associate, or organized health care arrangement in which the DoD covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted by the HIPAA Privacy Rule.
iii. A disclosure of PHI where a DoD covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Except as provided in the definition above, acquisition, access, use, or disclosure of PHI in a manner not permitted under this issuance is presumed to be a breach unless the DoD covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
2. The unauthorized person who used the PHI or to whom the disclosure was made.
3. Whether the PHI was actually acquired or viewed; and the extent to which the risk to the PHI has been mitigated.

A cybersecurity incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices, with respect to electronic PII/PHI. A cybersecurity incident may or may not involve a breach of PII/PHI. For example, a malware infection would be a possible breach if it could cause unauthorized access to PII/PHI. However, if the malware only affects data integrity or availability (not confidentiality), then a non-breach cybersecurity incident has occurred.

H.4.7.9.2 GENERAL

The breach response requirements shall be followed for all unauthorized use or disclosure of information regardless of whether the information is PHI or solely PII.

Because DoD defines "breach" to include possible (suspected), as well as actual (confirmed) breaches, the contractor shall implement these breach response requirements immediately upon the contractor's discovery of a possible breach. These procedures focus on the first two steps (breach identification and reporting) of a comprehensive breach response program, but also require addressing the remaining steps: containment, mitigation, which includes individual notification, eradication, recovery, and follow-up.

The contractor shall establish internal processes for carrying out the following procedures. These processes shall assign responsibility for investigating, classifying, reporting, and otherwise responding to breaches and cybersecurity incidents. The contractor shall consult with the DoD Privacy Office, where guidance is needed, when the contractor is uncertain whether a discovered breach is the contractor's responsibility (e.g., if the contractor discovers a breach not caused by the contractor), or how to classify an incident (breach vs. non-breach, confirmed vs. possible, or cyber vs. non-cyber). Under no circumstances shall a contractor delay reporting a confirmed or possible breach to the DoD Privacy Office beyond the 24-hour deadline while waiting for the DoD Privacy Office guidance or while investigating the incident. In conjunction with its initial investigation, the contractor shall immediately take steps to minimize any impact from the occurrence, proceed with further investigation of any relevant details (such as root causes, vulnerabilities exploited), and initiate further breach response steps.

In the event of a cybersecurity incident not involving a PII/PHI breach, the contractor shall follow applicable DoD cybersecurity and NIST requirements, which include United States-Computer Emergency Readiness Team (US-CERT) reporting (see **Section H.4.7.2**). If at any point a contractor finds that a cybersecurity incident involves a PII/PHI breach (possible or confirmed), the contractor shall immediately initiate the reporting procedures set forth below. The contractor shall also continue to follow any required cybersecurity incident response procedures and other applicable DoD cybersecurity requirements.

The contractor shall require subcontractors who discover a possible breach or cybersecurity incident to initiate the incident response requirements herein by reporting the incident to the contractor immediately after discovery. The time of that report to the contractor shall trigger the contractor's DHA Privacy Office reporting deadline (24 hours) under **Section H.4.7.9.1**. If a cybersecurity incident is involved, the contractor's deadline for US-CERT reporting (one hour) runs from the time the incident is confirmed. The contractor shall require the subcontractor to cooperate as necessary to meet these deadlines, maintain records, and otherwise enable the contractor to complete the breach response requirements herein. Alternatively, the contractor and subcontractor may agree that the subcontractor shall report directly to US-CERT and the DHA Privacy Office and the subcontractor shall be responsible for completing the response process, provided that such agreement requires the subcontractor to inform the contractor of the incident and the subsequent response actions.

The contractor shall maintain records of all breach and cybersecurity incident investigations, regardless of the outcome. Investigations identifying unauthorized disclosures must be logged for

HIPAA and Privacy Act disclosure accounting purposes, whether or not individual notification is required under the HIPAA Breach Rule.

The contractor, when acting as HIPAA-covered entities (rather than as business associates), the contractors are not subject to the breach response requirements herein. However, such contractors are subject to both the HIPAA Breach Rule (applicable to them in their capacity as covered entities) and DoD cybersecurity requirements (applicable to them in their capacity as DoD contractors).

H.4.7.9.3 REPORTING PROVISIONS

Immediately upon discovery of a possible or confirmed breach or cybersecurity incident, the contractor shall initiate an investigation. If the incident involves electronic PII/PHI, and if the investigation finds a confirmed breach or cybersecurity incident, the contractor shall report it, within one hour of confirmation, to the US-CERT Incident Reporting System at https://forms.us-cert.gov/report/, as required by the Department of Homeland Security (DHS).

Note: DHS no longer requires US-CERT reporting of non-cyber breaches or unconfirmed electronic breaches. However, DHS permits US-CERT reporting of unconfirmed cyber-related incidents on a voluntary basis. Thus, if a contractor is uncertain whether a possible cyber-related incident should be treated as confirmed and thus reportable, the contractor may voluntarily report the incident.

Before submission to US-CERT, the contractor shall save a copy of the on-line report. After submitting the report, the contractor shall record the US-CERT incident reporting number, which shall be included in the initial report to the DHA Privacy Office as described in this Section.

Note: Regardless of whether or not an incident is confirmed as a breach, the contractor shall also investigate whether or not the incident impacts data integrity or availability of PII/PHI. If such impact is confirmed, then the incident is reportable to US-CERT as a cybersecurity incident. For guidance on investigating the impact on data integrity and availability, refer to DoD cybersecurity and NIST guidance.

The contractor shall provide any updates to the initial US-CERT report by email to soc@us-cert.gov, and include the Reporting Number in the subject line. The contractor shall provide a copy of the initial or updated US-CERT report to the DHA Privacy Office if requested. Contractor questions about US-CERT reporting shall be directed to the DHA Privacy Office, not the US- CERT office.

In addition to US-CERT reporting, the contractor shall report a possible or confirmed breach to the DoD Privacy Office by submitting the form specified below within 24 hours of discovery of a breach (possible or confirmed), unless the breach falls within a category that the Privacy Office has determined to be not reportable. This 24-hour period runs from the time of discovery, unlike the one hour US- CERT reporting period, which runs from the time a cybersecurity incident is confirmed. Thus, depending on the time period needed to confirm, the report to the DoD Privacy Office may be due either before or after the US-CERT report.

The breach report form required within the 24-hour deadline shall be sent by e-mail to: DHA.PrivacyOfficer@mail.mil . The contractor shall also email the report to the FEDIM CO, the FEDIM COR, and OUSD (C) TPOCs. Encryption is not required because reports and notices shall not contain PII/PHI. If email is not available, telephone notification is also acceptable (at 703-725-6363), but all notifications and reports delivered telephonically must be confirmed in writing as soon as technically feasible.

Contractors shall prepare the breach reports required within the 24-hour deadline by completing the Breach Reporting DD Form 2959 (Breach of PII Report), available at the Breach Response link on the DoD Privacy Office web site, https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd2959.pdf. For non-cyber incidents without a US-CERT number, the contractor shall assign an internal tracking number and include that number in Box 1.e of the DD Form 2959. The contractor shall coordinate with the DHA Privacy Office for subsequent action, such as beneficiary notification and mitigation. The contractor shall promptly update the DD Form 2959 as new information becomes available.

When a Breach Report Form initially submitted is incomplete or incorrect due to unavailable information, or when significant developments require an update, the contractor shall submit a revised form or forms promptly after the new information becomes available, stating the updated status and previous report date(s) and showing any revisions or additions in red text. The contractor shall provide updates to the same parties as required for the initial Breach Report Form.

If the DHA Privacy Office determines that individual notification is required, the contractor shall provide written notification to beneficiaries affected by the breach as soon as possible, but no later than ten working days after the breach is discovered and the identities of the beneficiaries are ascertained. The ten-day period begins when the contractor is able to determine the identities (including addresses) of the beneficiaries whose records were impacted. If notification cannot be accomplished within ten working days, the contractor shall notify the DHA Privacy Office.

The contractor's proposed notification to be issued to the affected beneficiaries shall be submitted to the DHA Privacy Office for approval. The notification to beneficiaries shall include, at a minimum, the following:

a. Specific data elements.
b. Basic facts and circumstances.
c. Recommended precautions the beneficiary can take.
d. Federal Trade Commission (FTC) identity theft hotline information.
e. Any mitigation support services offered, such as credit monitoring.

Contractors shall ensure any envelope containing written notifications to affected individuals are clearly labeled to alert the recipient to the importance of its contents (e.g., "Data Breach Information Enclosed") and marked with the identity of the contractor and/or subcontractor organization that suffered the breach.

If media notice is required, the contractor shall submit a proposed notice and suggested media outlets for the DoD Privacy Office review and approval, which shall include coordination with the DHA Communications Division.

In the event the contractor is uncertain on how to apply the above requirements, the contractor shall consult with the DHA Privacy Office as appropriate when determinations on applying the above requirements are needed.

The contractor shall, at no cost to the Government, bear any costs associated with a breach of PII/PHI that the contractor has caused.

H.5 TRAINING AND PERMITS

All persons requiring routine access to OUSD(C) facilities or automated information networks, performing official travel on behalf of OUSD(C) as part of this TO, or performing unofficial travel shall complete initial Security Education and Awareness, Privacy Act, and Level I Antiterrorism Awareness Training provided by the OUSD(C). The DoD 5220.22-M, NISPOM, requires the contractor to provide security education and training to all cleared personnel annually. Refresher training shall reinforce the information provided during the initial security briefing and shall keep cleared personnel informed of appropriate changes in security regulations. The contractor shall report to the OUSD(C) TPOC and FEDSIM COR a form of acknowledgement that all contractor personnel have received refresher training. All other training the contractor personnel must have in the performance of their job that is not unique to the Government shall be performed at the contractor's expense and is not billable to the Government.

All contractors performing work in support of this TO shall comply with all OUSD(C) Security and Administrative policy and procedures. The contractor shall provide the OUSD(C) TPOC and FEDSIM COR documentation that all contractors have completed Intelligence Oversight training in accordance with DoD 5240.1-R prior to beginning work under this TO.

The contractor shall provide personnel with the appropriate certifications and/or training to perform the functional role assigned. The Government is not responsible for providing funding or training for contractor personnel to obtain a certification and/or to take training that would otherwise be required to perform that functional role. Exceptions to certification and training requests may be considered if the certification and training is not available to the general public. The contractor shall submit all exception requests to the FEDSIM COR and OUSD(C) TPOC for review and approval.

H.6 ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS

H.6.1 ORGANIZATIONAL CONFLICT OF INTEREST (OCI)

If a contractor has performed, is currently performing work, or anticipates performing work that creates or represents an actual or potential OCI, the contractor shall immediately disclose this actual or potential OCI to the FEDSIM CO in accordance with FAR Subpart 9.5. The nature of the OCI may involve the prime contractor, subcontractors of any tier, or teaming partners.

H.6.2 NON-DISCLOSURE REQUIREMENTS

If the contractor acts on behalf of, or provides advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, then the contractor shall execute and submit a

Corporate Non-Disclosure Agreement (NDA) Form (**Section J, Attachment L**) and ensure that all its personnel (including subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the TO:

a. Are instructed in the FAR 3.104 requirements for disclosure, protection, and marking of contractor bid or proposal information, or source selection information.
b. Are instructed in FAR Part 9 for third-party disclosures when acting in an advisory capacity.

All proposed replacement contractor personnel shall also be instructed in the requirements of FAR 3.104. Any information provided by contractors in the performance of this TO or obtained from the Government is only to be used in the performance of the TO. The contractor shall put in place appropriate procedures for the protection of such information and shall be liable to the Government for any misuse or unauthorized disclosure of such information by its personnel, as defined above.

H.7 SECTION 508 COMPLIANCE REQUIREMENTS

Unless the Government invokes an exemption, all Electronic and Information Technology (EIT) products and services proposed shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, 29 U.S.C. 794d, and the Architectural and Transportation Barriers Compliance Board's EIT Accessibility Standards at 36 CFR 1194. The contractor shall identify all EIT products and services provided, identify the technical standards applicable to all products and services provided, and state the degree of compliance with the applicable standards. Additionally, the contractor must clearly indicate where the information pertaining to Section 508 compliance can be found (e.g., Vendor's or other exact web page location). The contractor must ensure that the list is easily accessible by typical users beginning at TOA.

H.8 ADEQUATE COST ACCOUNTING SYSTEM

The adequacy of the contractor's accounting system and its associated internal control system, as well as contractor compliance with the Cost Accounting Standards (CAS), affect the quality and validity of the contractor data upon which the Government must rely for its management oversight of the contractor and Contract performance. The contractor's cost accounting system shall be adequate during the entire period of performance and shall permit timely development of all necessary cost data in the form required by the Contract.

H.9 APPROVED PURCHASING SYSTEM

The objective of a contractor purchasing system assessment is to confirm it is a Government-approved purchasing system and evaluate the efficiency and effectiveness with which the contractor spends Government funds and complies with Government policy with subcontracting. A Government-audited and approved purchasing system (e.g., approved by DCAA or Defense Contract Management Agency (DCMA)) is mandatory.

When reviews are conducted of the purchasing system during the performance of the TO, the contractor shall provide the results of the review to the FEDSIM CO within ten workdays from the date the results are known to the contractor.

H.10 EARNED VALUE MANAGEMENT (EVM)

The contractor shall employ EVM in the management of this TO in accordance with the American National Standards Institute (ANSI)/Electronic Industries Alliance (EIA) Standard-748-D-2019, *Earned Value Management Systems* (available at http://global.ihs.com/) and/or the guidelines established in the Performance Assessments and Root Cause Analyses (PARCA) publication *Agile and Earned Value Management: A Program Manager's Desk Guide*. The Government expects the contractor to employ innovation in its proposed application of EVM techniques to this TO in accordance with best industry practices.

The Government will conduct an Integrated Baseline Review within 120 calendar days after TOA, TO option periods, or incorporation of major TO modifications at the discretion of the Government or recommendation by the contractor. The objective of the Integrated Baseline Review is for the Government and the contractor to jointly assess areas, such as the contractor's planning, to ensure complete coverage of the TOR, logical scheduling of the work activities, adequate resources, and identification of inherent risks.

H.11 TRAVEL

H.11.1 TRAVEL REGULATIONS

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

a. FTR - prescribed by the GSA, for travel in the continental U.S.
b. JTR, Volume 2, DoD Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.
c. DSSR (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

H.11.2 TRAVEL AUTHORIZATION REQUESTS (TAR)

Before undertaking long-distance travel to any Government site or any other site in performance of this TO, the contractor shall have this long-distance travel approved by, and coordinated with, the FEDSIM COR. Notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long-distance travel, the contractor shall prepare a TAR (**Section J, Attachment M**) for Government review and approval. Long-distance travel will be reimbursed for cost of travel comparable with the FTR or JTR.

Requests for long-distance travel approval shall:

a. Be prepared in a legible manner.
b. Identify the TO number.
c. Identify the CLIN associated with the travel.
d. Contain the following:
    1. Itinerary containing date(s), time(s), and locations of origin and departure.
    2. Name of each contractor employee, company, and position title traveling.

3. Organization to be visited (if applicable).
4. Specific estimated costs (including airfare, rental car, lodging, transportation, parking, mileage, fuel, etc.) and applicable indirect cost rates.
5. Date the request to travel was communicated to the contractor from the Government.
6. Statement of travel purpose.

e. Be submitted at least 14 days in advance of the travel or within 48 hours of Government notification of travel, whichever is sooner, to permit review and approval by the Government.
f. Status of remaining CLIN funding.

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Long-distance travel shall be scheduled during normal duty hours whenever possible.

H.12 TOOLS (HARDWARE) AND ODCs

The Government may require the contractor to purchase hardware, software, and related supplies critical and related to the services being acquired under the TO. Such requirements will be identified at the time a TOR is issued or may be identified during the course of a TO by the Government or the contractor. If the contractor initiates a purchase within the scope of this TO and the prime contractor has an approved purchasing system, the contractor shall submit to the FEDSIM COR a RIP (**Section J, Attachment N**). If the prime contractor is to lose an approved purchasing system, the contractor shall submit to the FEDSIM CO a CTP (**Section J, Attachment O**). The RIP and CTP shall:

a. Be prepared in a legible manner.
b. Include the purpose of the purchase.
c. Specify the items being purchased.
d. Show the estimated cost of the purchase.
e. Include a cost comparison.
f. Show the rationale behind the purchase.

The contractor shall not make any purchases without an approved RIP from the FEDSIM COR or an approved CTP from the FEDSIM CO and without complying with the requirements of Section H.13.2.

H.13 COMMERCIAL SUPPLIER AGREEMENTS

H.13.1 The Government understands that commercial software that may be purchased in furtherance of this TO as described in **Sections C.5.2, C.5.3, C.5.4, and C.5.5** and as contemplated in the ODCs and Tools CLINs in **Section B.3** may be subject to commercial agreements that may take a variety of forms, including without limitation licensing agreements, terms of service, maintenance agreements, and the like, whether existing in hard copy or in an electronic or online format such as “clickwrap” or “browsewrap” (collectively, “Supplier Agreements”). The contractor shall provide all applicable Supplier Agreements to the FEDSIM CO prior to purchase and shall cooperate with the Government in negotiating suitable terms to comply with this Section which shall be “specific rights” pursuant to DFARS 227.7202-3.

H.13.2 The contractor shall ensure that any proposed Supplier Agreements allow the associated software and services to be used as necessary to achieve the objectives of this TO. The contractor shall provide all applicable Supplier Agreements to the FEDSIM CO prior to purchase and shall cooperate with the Government, including negotiations with the licensor as appropriate, to ensure compliance with this Section. Without limiting the generality of the foregoing, a compliant Supplier Agreement shall permit all of the following at no extra charge to the Government: (a) access and use by support contractors, including a successor contractor upon termination or expiration of this TO; (b) access and use by employees of other Federal, state, and local law enforcement agencies; (c) transfer to a different data center and/or a successor contractor's cloud; and (d) the creation of derivative works that shall be subject to at least the same rights as set forth in subparagraphs (a) through (c) above.

H.14 PRESS/NEWS RELEASE

The contractor shall not make any press/news release pertaining to this procurement without prior Government approval and only in coordination with the FEDSIM CO.

H.15 INTELLECTUAL PROPERTY RIGHTS

The existence of any patent, patent application, or other intellectual property right that encumbers any deliverable must be disclosed in writing on the cover letter that accompanies the delivery. If no such disclosures are provided, the data rights provisions in DFARS 252.227-7013 and 252.227-7014 apply.

H.16 AWARD FEE

See the AFDP in **Section J, Attachment D**.

H.17 CONTRACTOR IDENTIFICATION

As stated in 48 CFR 211.106, Purchase Descriptions for Service Contracts, contractor personnel shall identify themselves as contractor personnel by introducing themselves or being introduced as contractor personnel and by displaying distinguishing badges or other visible identification for meetings with Government personnel. Contractor personnel shall appropriately identify themselves as contractor employees in telephone conversations and in formal and informal written correspondence.

H.18 NATIONAL SECURITY AGENCY REQUIREMENTS

Technologies for OUSD(C) shall be procured in accordance with Committee on National Security Systems Policies (CNSSP) No. 11, "National Policy Governing the Acquisition of Information Assurance and IA-Enabled Information Technology Products." In addition, technologies shall be procured which have been validated by Common Criteria Testing Labs, in accordance with the National Information Assurance Partnership (NIAP) Protection Profiles (PPs). Where a PP exists but the desired product has not been validated against it, OUSD(C) shall direct the desired vendor to have its product validated against the appropriate, corresponding PP. For National Security Systems (NSS) where classified data is being protected at rest or in transit by commercial products, technologies from the Commercial Solutions for Classified (CSfC) Components List shall be used, in accordance with NSA's published CSfC

Capability Packages. Capability Packages and the CSfC Components List can be found by visiting the following website:

https://www.nsa.gov/resources/everyone/csfc/

NIAP-validated products can be found at the following NIAP website:

https://www.niap-ccevs.org/Product

H.19 ASSOCIATE CONTRACTOR AGREEMENTS (ACA)

Throughout the course of the TO, the contractor may be required to work with or within proximity to other contractors.

The contractor shall enter into an ACA with applicable third party developers and other stakeholders after TOA for any portion of the TO requiring joint participation in the accomplishment of the requirement. The agreements shall include the basis for sharing information, data, technical knowledge, expertise, and/or resources essential to this effort, which shall ensure the greatest degree of cooperation to meet the terms of the TO. The Government will provide specific names of other relevant contractors to the contractor.

ACAs shall include the following general information:

a. Identify the associate contractors and describe the relationships.
b. Identify the program involved and the relevant Government contracts of the associate contractors.
c. Describe the associate contractor interfaces by general subject matter.
d. Specify the categories of information to be exchanged or support to be provided.
e. Include the expiration date (or event) of the ACA.
f. Identify potential conflicts between relevant Government contracts and the ACA; include agreements on protection of proprietary data and restrictions on employees.

All costs associated with the ACAs shall be included in the negotiated cost of this TO. The contractor shall submit copies of all ACAs to the FEDSIM CO.

H.20 TECHNICAL DIRECTION LETTERS (TDLs)

A TDL is the means by which the Government will communicate technical direction concerning the details of the specific tasks set forth in the TO. Prior to commencement of any work, the Government will issue an approved TDL form **(Section J, Attachment I**), to the contractor, and a resulting TO funding modification will be provided when required. The TDL must be signed by the FEDSIM CO, FEDSIM COR, contractor, and OUSD(C) TPOC before work begins on the TDL.

Any TDL issued hereunder will be subject to the terms and conditions of the TO. The TO cannot be modified by the TDL; in the event of a conflict, the TO shall prevail. All TDLs must meet the following conditions:

a. The scope of services for any TDL must be contained in the current TO.
b. The supported office (i.e., OUSD(C)) must be identified in the current TO.

c. The TDL must be approved in writing by the OUSD(C) TPOC, FEDSIM COR, and FEDSIM CO prior to work commencement.

The Government will communicate TDLs in writing that will include, at a minimum, the following information:

a. TDL identification number.
b. Customer organization and POC information.
c. Funding organization and POC information (if different than customer).
d. TDL Title.
e. Severable designation.
f. Planned start date and duration of the TDL.
g. Task(s) under the TO that the TDL supports.
h. Description of work contained in the request, inclusive of expected outcomes and documentation requirements.

If the contractor does not agree with the estimated duration of the work specified on the TDL or considers the work to be outside the scope of the TO, the contractor shall notify the FEDSIM CO within three business days. The contractor shall undertake no performance to comply with the TDL until the matter has been resolved by the FEDSIM CO through a contract modification or other appropriate action.

I.1 TASK ORDER (TO) CLAUSES

All applicable and required clauses set forth in FAR 52.301 automatically flow down to all Alliant 2 TOs, based on their specific contract type (e.g., cost, fixed-price, etc.), statement of work, competition requirements, commercial or not commercial, and dollar value as of the date the TO solicitation is issued.

I.2 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This TO incorporates one or more clauses by reference with the same force and effect as if they were given in full text. Upon request, the FEDSIM CO will make their full text available. Also, the full text of a clause may be accessed electronically at the FAR website:

http://www.acquisition.gov/far/

FAR	TITLE	DATE
52.203-19	Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements	JAN 2017
52.204-19	Incorporation by Reference of Representations and Certifications	DEC 2014
52.204-21	Basic Safeguarding of Covered Contractor Information Systems	JUL 2016
52.216-7	Allowable Cost and Payment Fill-in: 30 days	AUG 2018
52.222-2	Payment for Overtime Premiums Fill-in: __$0__	JUL 1990
52.224-3	Privacy Training	JAN 2017
52.232-22	Limitation of Funds	APR 1984
52.232-40	Providing Accelerated Payments to Small Business Subcontractors	DEC 2013
52.239-1	Privacy or Security Safeguards	AUG 1996
52.246-5	Inspection of Services – Cost-Reimbursement	APR 1984

I.2.1 FAR CLAUSES INCORPORATED BY FULL TEXT

FAR 52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (AUG 2020)

(a) *Definitions.* As used in this clause—

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

Covered foreign country means The People's Republic of China.

Covered telecommunications equipment or services means–

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Critical technology means–

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

Interconnection arrangements means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Reasonable inquiry means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

Roaming means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) *Prohibition.* (1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(c) *Exceptions.* This clause does not prohibit contractors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement.

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information

in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

FAR 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed six months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days of the end of the period of performance.

(End of clause)

FAR 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

a. The Government may extend the term of this contract by written notice to the Contractor within 30 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

b. If the Government exercises this option, the extended contract shall be considered to include this option clause.

c. The total duration of this contract, including the exercise of any options under this clause, shall not exceed 66 months.

(End of clause)

I.3 GSAM CLAUSES INCORPORATED BY REFERENCE

The full text of a clause may be accessed electronically at the GSAM website:

https://www.acquisition.gov/gsam/gsam.html/

GSAM	TITLE	DATE
552.204-9	Personal Identity Verification Requirements	JUL 2020
552.232-25	Prompt Payment	NOV 2009
552.232-39	Unenforceability of Unauthorized Obligations (FAR Deviation)	FEB 2018
552.232-78	Commercial Supplier Agreements-Unenforceable Clauses	FEB 2018

I.4 DFARS CLAUSES INCORPORATED BY REFERENCE

The full text of a clause may be accessed electronically at Defense Pricing and Contracting website:

www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html

DFARS	TITLE	DATE
252.203-7000	Requirements Relating to Compensation of Former DoD Officials	SEP 2011
252.204-7009	Limitations on the Use or Disclosure of Third- Party Contractor Reported Cyber Incident Information	OCT 2016
252.204-7012	Safeguarding Covered Defense Information and Cyber Incident Reporting	DEC 2019
252.223-7004	Drug-Free Work Force	SEP 1988
252.227-7013	Rights in Technical Data Noncommercial Items	FEB 2014
252.227-7014	Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation	FEB 2014
252.227-7016	Rights in Bid or Proposal Information	JAN 2011
252.227-7019	Validation of Asserted Restrictions – Computer Software	SEP 2016
252.227-7028	Technical Data or Computer Software Previously Delivered to the Government.	JUN 1995
252.227-7030	Technical Data – Withholding of Payment	MAR 2000

252.227-7037	Validation of Restrictive Markings on Technical Data	SEP 2016
252.239-7001	Information Assurance Contractor Training and Certification	JAN 2008
252.239-7010	Cloud Computing Services	OCT 2016
252.242-7006	Accounting System Administration	FEB 2012
252.244-7001	Contractor Purchasing System Administration	MAY 2014
252.246-7001	Warranty of Data	MAR 2014

J.1 LIST OF ATTACHMENTS

The following attachments are attached, either in full text or electronically at the end of the TO.

ATTACHMENT	TITLE
A	COR Designation Letter (electronically attached.pdf)
B	Acronym List
C	Incremental Funding Chart (electronically attached .xls)
D	Draft Award Fee Determination Plan (AFDP)
E	Problem Notification Report (PNR) Template
F	Monthly Status Report (MSR) Template
G	Trip Report Template
H	Deliverable Acceptance-Rejection Report Template
I	Technical Direction Letter (TDL) Template
J	Department of Defense (DD) 254 (electronically attached .pdf)
K	Organizational Conflict of Interest (OCI) Statement (Removed)
L	Corporate Non-Disclosure Agreement (NDA) (Removed)
M	Travel Authorization Request (TAR) Template (electronically attached .xls)
N	Request to Initiate Purchase (RIP) Template (electronically attached .xls)
O	Consent to Purchase (CTP) Template (electronically attached .xls)
P	TPOC appointment letter(s) (To be provided upon award)